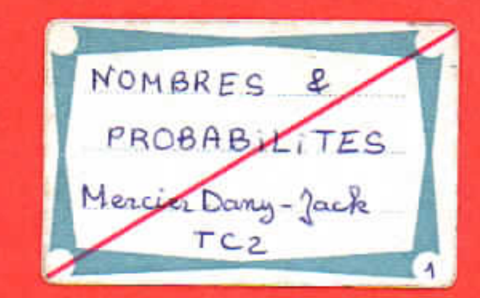




le Calligraphe

cahier ______________________

école ______________________

classe ______________________

nom ______________________



N° 103

001

TC2

NOMBRES & PROBABILITES

LEÇONS n° 1

COURS DE TERMINALE C

DE MME J. MAÑOTTE

recopié et présenté par D.-J. MERCIER

1974 - 75

19.9 1 Ensemble $\mathbb{N}$ des entiers naturels

(livre p 17)

$\exists \mathbb{N}$ tel que

1°/ + et × sont des lois internes dans $\mathbb{N}$. (voir propriétés)

2°/ $\leqslant$ exprime une relation d'ordre dans $\mathbb{N}$.

L'ordre est total :

$\forall (x, y) \in \mathbb{N}^2$, nous avons $x \leqslant y$ ou $y \leqslant x$

$x \in \mathbb{N}, y \in \mathbb{N}, z \in \mathbb{N}$

$x \leq y \longmapsto x + z \leqslant y + z$ (compatibilité)

3°/ $\forall A, A \subset \mathbb{N}$

$A \neq \emptyset, \exists \alpha, \alpha \in A \,/\, \forall x \in A, \alpha \leq x$

Ex : $\mathbb{N}$ a 0 comme plus petit élément.

4°/ $\forall A \subset \mathbb{N}$, $A \neq \emptyset$ et A majorée,

$\exists \beta \in A \,/\, \forall x \in A, \beta \geqslant x$. (cf p 18)

Ex : $\mathbb{N}$ n'a pas de plus grand élément.

Raisonnement par récurrence.

Soit $A \subset \mathbb{N} \,/\, 0 \in A$

et : $\forall x \in A \longmapsto x + 1 \in A$

Alors $A = \mathbb{N}$

Deuxième forme

$A \Delta B = (A-B) \cup (B-A)$

Soit $A = \{x \,/\, x \in \mathbb{N},\ \mathcal{P}(x) \text{ vraie}\}$

Si $\begin{cases} \mathcal{P}(0) \text{ est vraie.} \\ \mathcal{P}(n) \vdash \mathcal{P}(n+1) \end{cases}$

avec $n \in A$

Alors $\mathcal{P}(n)$ est générale = vraie $\forall n \in \mathbb{N}$.

Démonstration

$A \subset \mathbb{N}$; $B = \complement_{\mathbb{N}} A = \mathbb{N} - A$

Soit $y \in B$; $B = \{y,\ y \in \mathbb{N} \,/\, y \notin A\}$

Si $B \neq \emptyset$, $\exists y$ ($\exists$ = il existe au moins)

B est alors une partie non vide de $\mathbb{N}$; $\exists y_0$, le plus petit élément de B. $y_0 \neq 0$ car $0 \in A$ et $y_0 \in B$.

Donc, $\exists (y_0 - 1)$

$y_0 - 1 \in A$ car y_0 est le p.p. élément de B.

Or, $y_0 - 1 \in A \vdash (y_0 - 1) + 1 \in A$ (voir énoncé)

$\vdash y_0 \in A$

Or, $A \cap B = \emptyset$, d'où contradiction : c'est donc que $B = \emptyset$ ($\nexists y$) $\vdash A = \mathbb{N}$

Exemple.

Montrer que :

$1 + 3 + 5 + \dots + (2n-1) = n^2 \quad : \mathcal{P}(n)$

1°/ $\mathcal{S}(1)$ est vraie car $1 = 1^2$

2°/ $\mathcal{S}(n) \vdash \mathcal{S}(n+1)$?

Si $1 + 3 + 5 + \dots + (2n-1) = n^2$,

alors est-ce que :

$$\underbrace{1 + 3 + 5 + \dots + (2n-1)}_{n^2} + (2n+1) = (n+1)^2 \quad ?$$

$$n^2 + (2n+1) \qquad = n^2 + 2n + 1$$

Conclusion :

$\mathcal{S}(n)$ est vraie $\forall n \in \mathbb{N}^*$

26.9 Remarque.

Si $0 \notin A \mapsto$ Si $\mathcal{S}(0)$ non vraie,

Si, de plus, le 1er élément de $\mathbb{N}$ pour lequel $\mathcal{S}(x)$ est vraie est $\boxed{a}$

$$\begin{cases} \mathcal{S}(a) \text{ vraie} \\ \quad\text{et} \\ \mathcal{S}(x) \vdash \mathcal{S}(x+1) \text{ vraie} \end{cases}$$

Alors $\mathcal{S}(x)$ vrai $\forall x \in \mathbb{N} - \{0, 1, \dots, a-1\} = A$

26.9 2 Principe des systèmes de numération.

1°/ Propriété d'Archimède :

$a \in \mathbb{N}$, $b \in \mathbb{N}^*$

$(a+1)\,b = ab + b$

$\begin{cases} (a+1)\,b > ab & (\text{car } b > 0) \\ ab \geqslant a & \text{car } (b \geqslant 1) \end{cases}$

donc :

$(a+1)b > a$

$a < \underbrace{(a+1)}b$

$\boxed{\exists k \in \mathbb{N}}$; $a < kb$

L'ensemble des entiers tels que k n'est pas vide puisque a + 1 est l'un d'entre eux

∃ un plus petit élément dans cette partie ≠ ∅ de ℕ.

On l'appelle q + 1. Son prédécesseur dans ℕ est q et ne vérifie pas $a < kb$

nous avons donc : $a \geqslant qb$

On rappelle $a < (q+1)b$

(1) $\boxed{qb \leqslant a < (q+1)b}$

ex : $25 \times 5 \leqslant a < 26 . 5$

$25 = q =$ quotient entier de a par 5 si et seulement si $a = 125$, ou 126, ou 127, ou 129.

Reste de la division euclidienne de a par b :

c'est $r \in \mathbb{N}$ / $a = bq + r$

$r = a - bq$; $r \geqslant 0$ et $r < b$

$r = a - bq$ $0 \leqslant r < b$

(2) $\quad (a = bq + r)$

Les propriétés (1) et (2) sont équivalentes.

27.9 2°/ Écriture d'un entier naturel n dans un système de numération de base x.

Le principe est le même que si $x = 10$:

a) Si $n < x$, on écrit n avec un symbole unique appelé "chiffre" (ou un caractère)

b) Si $n \geqslant x$, on écrit n à l'aide de chiffres rangés dans un ~~nombre~~ ordre tel que : à droite, le nombre des unités simples.

à sa gauche, le nombre des unités du 2e ordre, chacune d'elle renferment x unités simples.

* encore à sa gauche, le nombre des unités du 3e ordre, chacune renferment x unités du 2e ordre.

* ...

Pratique

1°/ $n < x$, on convient d'un choix de x caractères

* $x \leq 10$, on utilise les chiffres habituels.
* $x > 10$, on en introduit de nouveaux en gardant les dix premiers.

ex : x = douze ; $\{0, 1, \dots, 9, \alpha, \beta\}$

2°/ $n \geqslant x$, on div $\exists (q_1, r_1)$ /

$n = \boxed{q_1} x + \boxed{r_1}$, $0 \leq r_1 < x$ $(x \neq 0)$

* Si $q_1 < x$, on convient d'écrire :

$$n = \overline{q_1 r_1}$$

* Si $q_1 \geqslant x$, on le divise à son tour par x :

$q_1 = q_2 x + r_2$ $\quad 0 \leq r_2 < x$

* Si $q_2 < x$, on convient d'écrire :

$n = \overline{q_2 r_2 r_1}$

* Si $q_2 \geqslant x$,

$q_2 = q_3 x + r_3$ $\quad 0 \leqslant r_3 < x$

et ainsi de suite.

et $n = \overline{q_p r_p \dots r_1}$

Résumé

	$n = q_1 x + r_1$	$0 \leq r_1 < x$
$\times x$	$q_1 = q_2 x + r_2$	$0 \leq r_2 < x$
$\times x^2$	$q_2 = q_3 x + r_3$	$0 \leq r_3 < x$
	- - - - - - - - - -	
$\times x^{p-1}$	$q_{p-1} = q_p x + r_p$	$0 \leq r_p < x$
$\times x^p$	$q_p = 0 x + q_p$	$0 < q_p < x$

Si $q_p = r_{p+1} \neq 0$

On ajoute membre à membre les égalités obtenues après les multiplications prévues:

$$n = r_1 + r_2 x + r_3 x^2 + \dots + r_p x^{p-1} + \underbrace{q_p}_{r_{p+1}} x^p$$

$$\boxed{n = r_{p+1} x^p + r_p x^{p-1} + \dots + r_2 x + r_1.}$$ base dix

$$\boxed{n = \overline{r_{p+1}\, r_p \dots r_2\, r_1}}$$ base x

Exemple

Si $x = 2$ (base deux).

$n_x = 10010111101$

$n = 1x^{10} + 1x^7 + 1x^5 + 1x^4 + 1x^3 + 1x^2 + 1$

$= 1024 + 128 + 32 + 16 + 8 + 4 + 1$

$n = 1213$ (base dix)

Écriture de la base x dans la base x.

$x^1 = 1x^1 + 0$

$x = \overline{10}$, en base x, $\forall x \in \mathbb{N} - \{0, 1\}$

$x^2 = \overline{100}$

Unicité de l'écriture de $n \in \mathbb{N}$ dans un système de

$\exists ! (q_1, r_1)$; $\exists ! (q_2, r_2)$; ...

De plus, la position des restes successifs est imposée.

Remarque

$x = \overline{10}$ $\forall x$

$x^2 = \overline{100}$

$x^n = \underbrace{\overline{100...00}}_{n+1 \text{ caractères}}$

mais n zéros.

2.10 3 Étude de l'anneau $(\mathbb{Z}, +, \times)$

Il s'agit de $(\mathbb{Z}, +, \times)$

1°/ $(\mathbb{Z}, +)$ groupe commutatif.
2°/ $\times$ est associative.
3°/ $\times$ est distributive sur
} $\mathbb{Z}$ est un anneau.

4°/ $\mathbb{Z}$ est un anneaux commutatif

5°/ $\mathbb{Z}$ " " unitaire

Étude de $E = n\mathbb{Z}$, $n \in \mathbb{N}$.

$E = \{x \in \mathbb{Z} \,/\, \exists q \in \mathbb{Z} , x = nq\}$

3.10 $(E, +)$ est un sous-groupe de $(\mathbb{Z}, +)$:

1°) $E \neq \emptyset$ car $0 = n.0$ donc $0 \in n\mathbb{Z}$

2°/ $x \in n\mathbb{Z}$ et $x' \in n\mathbb{Z}$

$x - x' = nq - nq' = n(q - q')$

$q \in \mathbb{Z}$, $q' \in \mathbb{Z}$ $\quad q - q' \in \mathbb{Z}$

$[q + (-q') \in \mathbb{Z}]$

$\exists\ q - q' = Q \in \mathbb{Z} \,/\, x - x' = nQ$

$x - x' \in n\mathbb{Z}$

Inversement, soit E un sous-groupe de $(\mathbb{Z}, +)$.

1°/ Si $E = \{0\}$, il peut se mettre sous la forme $E = n\mathbb{Z}$

2°/ Si $E \neq \{0\}$, alors $\exists \underset{\neq 0}{x} \in E$, $\exists (-x) \in E$

Des deux : x et $-x$, l'un est positif. L'ensemble des entiers positifs inclu dans E n'est pas vide, soit

$A \neq \emptyset$ et $A \subset \mathbb{N} \mapsto \exists$ plus petit élément dans A

soit n cet élément.

* Considérons $E' = n\mathbb{Z}$ $(n \in \mathbb{N}^*)$

$n\mathbb{Z} \subset E$?

$$x = \underbrace{n}_{\in E} q$$

Si $q > 0$, $x = \underbrace{\underbrace{n + n + \dots + n}_{q \text{ termes}}}_{\in E}$ (+ interne dans E)

Si $q < 0$, $-q = q' > 0$

$x = nq = \underbrace{(-n)}_{\in E}\underbrace{q'}_{>0}$ et $x \in E$ aussi.

Si $q = 0$, $x = 0 \in E$.

Donc $n\mathbb{Z} \subset E$

* On n'aura $n\mathbb{Z} = E$ que si, de plus $E \subset n\mathbb{Z}$

Si $x \in E$, $x = nq + r$ $\quad 0 \leqslant r < \underbrace{n}_{\text{diviseur}}$

Si $r > 0$, $r = \underbrace{x}_{\in E} - \underbrace{nq}_{\in E \text{ (cf } n\mathbb{Z} \subset E)}$

Donc $r \in E$

Or, n est le plus petit élément strictement positif de E. Donc :

incompatibilité avec $0 < r < n$.

Donc $r = 0 \longmapsto x = nq \in n\mathbb{Z}$

Donc $E \subset n\mathbb{Z}$

* Conclusion

"Tous les sous-groupes de $(\mathbb{Z},+)$ sont de la forme $(n\mathbb{Z},+)$."

Sous-anneaux de $(\mathbb{Z},+,\times)$

Ce sont des sous-groupes de $(\mathbb{Z},+)$ donc des $n\mathbb{Z}$.

Tous les $n\mathbb{Z}$ sont-ils anneaux ? oui si et seulement si

$\forall x \in n\mathbb{Z}$, $\forall x' \in n\mathbb{Z}$, alors $x \times x' \in n\mathbb{Z}$

Or, $x.x' = nq.nq' = n\underbrace{(qnq')}_{\in \mathbb{Z}} = nQ$

$xx' \in n\mathbb{Z}$.

"Tous les sous-anneaux de $(\mathbb{Z},+,\times)$ sont les $n\mathbb{Z}$"

4.10

Définition d'un idéal d'un anneau commutatif

$(A,+,\times)$ = anneau commutatif

I = idéal de A si et seulement si :

* $(I, +)$ = sous-groupe
* $\forall x \in I$, $\forall y \in A$, $x \times y \in I$

On dit que I est (2e propriété) une partie "multiplicativement permise" de A.

Résumé :

* $\forall (x,y) \in I^2$, $x - y \in I$
* $\forall x \in I$, $\forall z \in A$, $x \times z \in I$

Cas où $A = \mathbb{Z}$

Les idéaux de $\mathbb{Z}$ sont évidemment les $n\mathbb{Z}$ car

1°) $n\mathbb{Z}$ = sous-groupe de $\mathbb{Z}$

2°) $\forall x = nq$, $q \in \mathbb{Z}$

$\forall z \in \mathbb{Z}$ $\quad x z = n \underbrace{(q z)}_{\in \mathbb{Z}}$

$$x z = n q' \in n\mathbb{Z}$$

Diverses expressions

1) a est divisible par $b \neq 0$

2) a est multiple de b.

3) b divise a : $b \mid a$

4) b est diviseur de a.

Cela signifie : $a \in \mathbb{Z}$, $b \in \mathbb{Z}$,

$\exists\, q \in \mathbb{Z} \;/\; a = bq$

5) $a\mathbb{Z} \subset b\mathbb{Z}$

Ex : $3 \mid 15$; tout multiple de 15 est multiple de 3 ; la réciproque est fausse.

$b \mid a \longmapsto (a) \subset (b)$

$(a) = a\mathbb{Z}$

$(b) = b\mathbb{Z}$.

(a) se lit " Idéal de a ".

7.10

Etude de l'ensemble $\mathbb{Z}/n\mathbb{Z}$

1°/ Division euclidienne de $a \in \mathbb{Z}$ par $b \in \mathbb{N}^*$

α) Si $a \geqslant 0$ ($a \in \mathbb{N}$), déjà vu :

$$bq \leqslant a < b(q+1)$$

ou : $a = bq + r \quad 0 \leqslant r < b$

β) Si $a \leqslant 0$ ($a \in \mathbb{Z}_-$) ; $a = -a' \quad a' \in \mathbb{N}$

$$bq' \leqslant a' < b(q'+1)$$

* si $a' = bq'$, alors $a = -a' = -b\,q' = b\underbrace{(-q')}_{\in \mathbb{Z}}$

donc $a = b\underbrace{(-q')}$

quotient de a par b.

ex : $a = -35$; $b = 7$ $\qquad -35 = 7 \times \underbrace{(-5)}_{-q'}$

$-q' = q$ = quotient de a par b.

* $a' \neq bq'$

$$bq' < a' < b(q'+1)$$

$$-b(q'+1) < \underbrace{-a'}_{a} < -bq'$$

$$-b(q'+1) < a < -bq'$$

$$b\underbrace{[-(q'+1)]}_{q} < a < b\underbrace{(-q')}_{q+1}$$

$b\,\boxed{q} < a < b(q+1)$

q est le quotient entier de a par b.

ex : $7 \times \underbrace{\boxed{(-6)}}_{q} < \underbrace{-37}_{a} < \underbrace{7}_{b} \times (-5)$

$-37 = 7(-6) + \underbrace{5}$

$r \geqslant 0$, $+r < 7$

$$a = bq + r \qquad 0 \leqslant r < b$$

2°/ Relation d'équivalence dans $\mathbb{Z}$.

$\forall (x, y) \in \mathbb{Z}^2$, $x \mathcal{R} y \longmapsto x - y \in n\mathbb{Z}$

ex : $n = 5$, $x = -37$

$y = -57$

$x - y = -37 + 57 = 20 \in n\mathbb{Z}$

$x - y \in 5\mathbb{Z} \longmapsto x \mathcal{R} y$.

* $\forall x \in \mathbb{Z}$ $\quad x \mathcal{R} x$?

$x \mathcal{R} x \longmapsto x - x \in n\mathbb{Z}$

Or $x - x = 0 \in n\mathbb{Z}$, oui.

* $\forall (x, y) \in \mathbb{Z}^2$, $x \mathcal{R} y \longmapsto y \mathcal{R} x$?

$x \mathcal{R} y \longmapsto x - y \in n\mathbb{Z}$

$(n\mathbb{Z}, +)$ = groupe $\vdash$ $y - x \in n\mathbb{Z}$.

$\vdash$ $y \mathcal{R} x$

• $\forall (x, y, z) \in \mathbb{Z}^3$.

$$\left.\begin{matrix} x \mathcal{R} y \\ y \mathcal{R} z \end{matrix}\right\} \vdash x \mathcal{R} z \ ?$$

$x - y \in n\mathbb{Z}$

$y - z \in n\mathbb{Z}$

$\underbrace{x - z} \in n\mathbb{Z}$

somme de 2 éléments de $n\mathbb{Z}$.

oui, $x \mathcal{R} z$.

Donc $\mathcal{R}$ est relation d'équivalence ; elle permet de définir des classes

Une classe = $\{ y \ ; \ y \in \mathbb{Z} \ / \ x \mathcal{R} y$, x étant l'élément choisi pour reconnaître la classe$\}$

Tous les éléments de $\mathbb{Z}$ peuvent être ainsi classés et l'ensemble des classes ou ensemble-quotient de $\mathbb{Z}$ par la relation $\mathcal{R}$ que l'on note $\mathbb{Z} / n\mathbb{Z}$ va être étudié :

ex : $n = 3$

Pour placer tout entier relatif dans une classe et une seule, utilisons le théorème suivant :

$x-y \in n\mathbb{Z} \longmapsto$ x et y donnent le même reste dans la division par n.

En effet :

* $x = nq + r \qquad 0 \leq r < n$

$\underline{y = nq' + r}$

$x - y = \underbrace{n}_{\in \mathbb{N}^*} \underbrace{(q-q')}_{\in \mathbb{Z}}$ car $(q, q') \in \mathbb{Z}^2$

* $x - y \in n\mathbb{Z}$

On divise x par n : $\underline{x = nq + r} \qquad 0 \leq r < n$

or $x - y = nq'$

$y = x - nq' = (nq + r) - nq'$

$= n\underbrace{(q-q')}_{\in \mathbb{Z}} + r$

$\underline{y = nk + r} \qquad 0 \leq r < n$

r = reste de y par n.

Revenons à la recherche des classes de $\mathbb{Z}/3\mathbb{Z}$:

1°/ $r = 0$, $x = \{^{3}_{nq}$ $\quad \forall q \in \mathbb{Z}$

2°/ $r = 1$, $x = nq + 1$

3°/ $r = 2$, $x = nq + 2$

Tous les $x \in \mathbb{Z}$ ont été classés.

$\mathbb{Z}/3\mathbb{Z} = \{$ cl de 0 ; cl de 1 ; cl de 2 $\}$

$\mathbb{Z}/3\mathbb{Z} = \{\dot{0} ; \dot{1} ; \dot{2}\}$

$$\mathbb{Z}/n\mathbb{Z} = \{\underbrace{\dot{0} ; \dot{1} ; \dots ; \widehat{n-1}}_{n \text{ classes}}\}$$

Si $n = 5$, $\left.\begin{array}{l} -37 \in \dot{3} \\ -57 \in \dot{3} \end{array}\right\} \dot{3} \in \mathbb{Z}/5\mathbb{Z}$

$\dot{3} \subset \mathbb{Z}$

$20 \in \dot{0}$

On dit que -37 et -57 sont congrus modulo 5

20 et -75 " " "

On écrit :

$-37 \equiv -57 \ [5]$

$+20 \equiv -75 \ (\text{mod. } 5)$

$45 \equiv 0 \ [5]$

8.10

Compatibilité de + et de $\mathcal{R}$.

de x et de $\mathcal{R}$

1°/ $x \equiv x' \ [n]$

$y \equiv y' \ [n]$

$x + y \equiv x' + y' \ [n]$?

oui car $x - x' \in n\mathbb{Z}$, $y - y' \in n\mathbb{Z}$

$(x-x') + (y-y') \in n\mathbb{Z}$ $\quad$ $n\mathbb{Z}$ est un sous-groupe

$(x+y) - (x'+y') \in n\mathbb{Z}$

$x+y \equiv x'+y' \; [n]$

$x' \in \dot{x} \quad , \quad y' \in \dot{y}$

$x'+y' \in \dot{\overline{x+y}}$

2°/ $x \times y \equiv x' \times y' \quad [n]$

Or, $\quad x = x' + nk \quad k \in \mathbb{Z}$

$y = y' + nk' \quad k' \in \mathbb{Z}$

$$xy = x'y' + n(\underbrace{ky' + k'x' + nkk'}_{K \in \mathbb{Z}})$$

$xy = x'y' + nK$

$xy \equiv x'y' \; [n]$

$x' \in \dot{x} \quad , \quad y' \in \dot{y}$

$x'y' \in \dot{\overline{xy}}$

Opérations $\dot{+}$ et $\dot{\times}$ dans $\mathbb{Z}/n\mathbb{Z}$

Définition

$\dot{x} \dot{+} \dot{y} = \dot{\overline{x+y}}$

$\dot{x} \dot{\times} \dot{y} = \dot{\overline{x \times y}}$

Homomorphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$x \longmapsto \dot{x} = f(x)$$
$$y \longmapsto \dot{y} = f(y)$$
$$\underbrace{x+y}_{z} \longmapsto \underbrace{\dot{x} \dot{+} \dot{y}}_{\dot{z}} = f(z)$$

$$\boxed{f(x+y) = f(x) \dot{+} f(y)}$$

f est un homomorphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$

De plus f est surjective :

$\forall \dot{x} \in \mathbb{Z}/n\mathbb{Z}, \ \exists x, x \in \mathbb{Z} / \ f(x) = \dot{x}$

f = homomorphisme surjectif.

De même :

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$x \longmapsto \dot{x} = f(x)$$
$$y \longmapsto \dot{y} = f(y)$$

$$x \times y \longmapsto \underbrace{\dot{x}}_{f(x)} \dot{\times} \underbrace{\dot{y}}_{f(y)} = f(x \times y)$$

$$\boxed{f(x \times y) = f(x) \dot{\times} f(y)}$$

f est un homomorphisme surjectif de $(\mathbb{Z}, \times)$ sur $(\mathbb{Z}/n\mathbb{Z}, \dot{\times})$

Structure de $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$

9 10 1°/ $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ groupe commutatif.

* $\forall (\dot{x}, \dot{y}, \dot{z}) \in (\mathbb{Z}/n\mathbb{Z})^3$, a-t-on :

$(\dot{x} \dot{+} \dot{y}) \dot{+} \dot{z} = \dot{x} \dot{+} (\dot{y} \dot{+} \dot{z})$?

$\overset{\cdot}{\overline{x+y}} \dot{+} \dot{z} = \dot{x} \dot{+} \overset{\cdot}{\overline{y+z}}$?

$\overset{\cdot}{\overline{(x+y)+z}} = \overset{\cdot}{\overline{x+(y+z)}}$?

+ est associative dans $\mathbb{Z}$, donc la réponse est oui.

* $\exists \dot{0} \in \mathbb{Z}/n\mathbb{Z} \;/\; \forall \dot{x} \in \mathbb{Z}/n\mathbb{Z}$,

$\underbrace{\dot{x} \dot{+} \dot{0}}_{\overset{\cdot}{\overline{x+0}}} = \underbrace{\dot{0} \dot{+} \dot{x}}_{\overset{\cdot}{\overline{0+x}}} = \dot{x}$

(0 neutre dans $(\mathbb{Z}, +)$)

* $\forall \dot{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists \dot{\overline{-x}} \in \mathbb{Z}/n\mathbb{Z}$

$\underbrace{\dot{x} \dot{+} \dot{\overline{-x}}}_{\overset{\cdot}{\overline{x-x}}} = \dot{\overline{-x}} \dot{+} \dot{x} = \dot{0}$

* $\forall \dot{x} \in \mathbb{Z}/n\mathbb{Z}$, $\forall \dot{y} \in \mathbb{Z}/n\mathbb{Z}$

$\dot{x} \dot{+} \dot{y} = \dot{y} \dot{+} \dot{x}$

$\overline{x+y} = \overline{y+x}$

oui.

2/ $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$

* $\forall (\dot{x}, \dot{y}, \dot{z}) \in (\mathbb{Z}/n\mathbb{Z})^3$

$(\dot{x} \dot{\times} \dot{y}) \dot{\times} \dot{z} = \dot{x} \dot{\times} (\dot{y} \dot{\times} \dot{z})$?

$\dot{\overline{xy}} \dot{\times} \dot{z} = \dot{x} \dot{\times} \dot{\overline{yz}}$

$\overline{(xy) \times z} = \overline{x(yz)}$

$\overline{xyz} = \overline{xyz}$ oui.

* $(\dot{x} \dot{+} \dot{y}) \dot{\times} \dot{z} = \dot{x} \dot{\times} \dot{z} \dot{+} \dot{y} \dot{\times} \dot{z}$?

distributivité à droite.

$\dot{\overline{x+y}} \dot{\times} \dot{z} = \dot{\overline{xz}} \dot{+} \dot{\overline{yz}}$

$\overline{(x+y) \times z} = \overline{xz + yz}$

oui

* $\forall \dot{x} \in \mathbb{Z}/n\mathbb{Z}$; $\dot{x} \dot{\times} \dot{1} = \dot{1} \dot{\times} \dot{x} = \dot{x}$

$\overline{x.1} = \overline{1.x} = \dot{x}$

* $\dot{x} \dot{\times} \dot{y} = \dot{y} \dot{\times} \dot{x}$?

$\dot{\overline{xy}} = \dot{\overline{yx}}$, oui.

$(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$: anneau commutatif unitaire.

De plus, il se peut que $\forall \dot{x} \in \mathbb{Z}/n\mathbb{Z} - \{\dot{0}\}$, il existe $\dot{x}' \in (\mathbb{Z}/n\mathbb{Z})^* / \dot{x} \times \dot{x}' = \dot{1}$

$\dot{x}'$: classe inverse de $\dot{x}$.

Mais ce n'est pas général.

Si cela est vrai, alors $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe multiplicatif

$n = 5$

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

$n = 6$

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

$(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$ = corps commutatif.

$(\mathbb{Z}/6\mathbb{Z}, \dot{+}, \dot{\times})$ = anneau unitaire commutatif.

Remarque.

$(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$ = anneau intègre :

$\dot{x} \dot{\times} \dot{y} = \dot{0} \vdash \dot{x} = \dot{0}$ ou $\dot{y} = \dot{0}$

1°/ (voir table).

2°/ Toute classe, sauf $\dot{0}$, est <u>inversible</u> :

$\forall \dot{x} \neq \dot{0}, \ \exists \dot{x}' \ / \ \dot{x} \dot{\times} \dot{x}' = \dot{1}$

$G \quad \underbrace{\dot{x}' \dot{\times} \dot{x}}_{\dot{1}} \dot{\times} \dot{y} = \dot{x}' \dot{\times} \dot{0}$

$\dot{1} \dot{\times} \dot{y} = \dot{0} \vdash \dot{y} = \dot{0}$

démonstra[tion] généra[le]

4 10 5 Rappel : $a|b$. PGCD

$a|b \Rightarrow b\mathbb{Z} \subset a\mathbb{Z}$

1°) $a|a$ oui (Réflexivité)

2°) $a|b$ et $b|a \Rightarrow a = b$ (Antisymétrie)

3°) $a|b$ et $b|c \Rightarrow a|c$ (Transitivité)

La relation $|$ (se lit "divise") est relation d'ordre.

L'inclusion aussi :

* $A \subset A$, $\forall A \in E$
* $A \subset B$ et $B \subset A \Rightarrow A = B$
* $A \subset B$ et $B \subset C \Rightarrow A \subset C$

Remarque

$|$ est d'ordre dans $\mathbb{N}$

mais, dans $\mathbb{Z}$, l'antisymétrie n'est pas réalisée :

$1|-1$ et $-1|1$ et pourtant $1 \neq -1$

De plus, les 2 relations sont d'ordre partiel.

Somme de deux idéaux

$(a) = a\mathbb{Z}$, $a \neq 0$

$(b) = b\mathbb{Z}$, $b \neq 0$

$J \subset \mathbb{Z}$ / $J = \{x, x \in \mathbb{Z} / \boxed{\exists} (u, v) \in \mathbb{Z}^2 :$
$x = au + bv\}$

1°/ $J \neq \emptyset$ (voir $0, a, b \in J$)

$\forall x \in J, \forall y \in J, \quad x - y \in J$?

$$\begin{cases} x = au + bv \\ y = au' + bv' \end{cases}$$

$$x - y = a\underbrace{(u - u')}_{\in \mathbb{Z}} + b\underbrace{(v - v')}_{\in \mathbb{Z}} \in J$$

$(J, +)$ sous-groupe de $\mathbb{Z}$.

2°/ $\forall x \in J, \forall z \in \mathbb{Z}, \quad x.z \in J$?

$$(au + bv)z = a\underbrace{(uz)}_{\in \mathbb{Z}} + b\underbrace{(vz)}_{\in \mathbb{Z}} \in J$$

J est partie " multiplicativement permise " de $\mathbb{Z}$

J = idéal de $\mathbb{Z}$.

$J = (a) \boxed{+} (b)$

$\exists \delta > 0$ si et seulement si $J \neq \{0\}$

Or, $a \in J$ et $a \neq 0$

Donc $J \neq \{0\}$, donc $\delta > 0$ et $\boxed{J = \delta\mathbb{Z}}$

Comparaison de δ et a :

$a = a.1 + b.0 \in J$

$a = \delta q \vdash$ $\boxed{\delta \mid a}$

$(a) \subset (\delta)$ (ou $a\mathbb{Z} \subset \delta\mathbb{Z}$ ou $(a) \subset J$)

De même $(b) \subset (\delta)$

$\boxed{\delta \mid b}$

De plus, $\delta \in \delta\mathbb{Z}$

$\exists (u_0, v_0) \in \mathbb{Z}^2 /$ $\boxed{\delta = a u_0 + b v_0}$

Conséquence

Tout $d \in \mathbb{Z}$ tel que $d \mid \delta$ est tel que d / a

De même $d \mid b$.

Tout diviseur de δ divise a et b

Inversement, tout d' qui divise a et b permet d'écrire : $a = d'q \quad , q \in \mathbb{Z}$

$b = d'q_1 \quad , q_1 \in \mathbb{Z}$

et $\delta = d'q u_0 + d'q_1 v_0$

$$\delta = d'\underbrace{(qu_0 + q_1 v_0)}_{\in \mathbb{Z}} \quad \vdash \quad d' \mid \delta$$

Tout diviseur commun à a et b divise δ

d divise a et b $\longmapsto$ d divise δ
$d \in \mathbb{Z}$

Remarque : $a \in \mathbb{N}^*$, $b \in \mathbb{N}^*$ et $\delta \in \mathbb{N}^*$
Dans le cas où $\delta = 1$, on dit que a et b sont premiers entre eux :
$1 = a u_0 + b v_0$
"Si" a et b sont premiers entre eux" équivaut à :
" $\exists (u_0, v_0) \in \mathbb{Z}^2$ / $a u_0 + b v_0 = 1$ ".

21.10 L'entier naturel δ évoqué dans ce qui précède n'est autre que le plus grand des diviseurs communs à a et b (a et b entiers relatifs ; souvent naturels)
$\delta =$ PGCD de a et b
$\delta = \Delta(a, b) = a \wedge b$

Si $\Delta(a, b) = 1$, a et b sont dits premiers entre eux sont $+1$ et -1.
$a u_0 + b v_0 = 1$ est dite "égalité de Bezout".

ex : $a = +6$, $b = -7$
$\exists$ $u_0 = 13$; $v_0 = 11$ / $6 \times 13 + (-7) \times 11 =$

En effet $78 - 77 = +1$

$\Delta(6, -7) = +1$

Propriétés du PGCD de a et b.

1°/ $\delta = \Delta(a, b)$, $(a, b) \in \mathbb{Z}^{*2}$

$\delta' = \Delta(ca, cb)$, $c \in \mathbb{Z}^*$

$\delta' \mathbb{Z} = (\delta') = \{x, x \in \mathbb{Z} / \exists (u, v) \in \mathbb{Z}^2, x = ca.u + cb.v\}$

Or, $x = c(au + bv)$

$au + bv$ est élément de (δ), et inversement, tout élément de (δ) est de cette forme. De plus, tout $x \in \delta' \mathbb{Z}$ est multiple de c. Donc, le plus petit entier positif de $\delta' \mathbb{Z}$ est $(|c|.\delta)$; or, c'est δ' par définition :

$$\boxed{\delta' = |c|.\delta} \quad (1)$$

2°/ $\delta = \Delta(a, b)$

Soit d un diviseur commun à a et b.

$a = d a'$, $b = d b'$, $(a', b') \in \mathbb{Z}^{*2}$

$\delta' = \Delta(a', b')$

$\delta = \Delta(a'd, b'd) = \Delta(a, b)$

donc : (cf 1°/ $\delta = \delta'.|d|$ donc :

$$\boxed{\delta' = \frac{\delta}{|d|}} \quad (2)$$

Conséquence

Prenons $d = \delta = \Delta(a, b)$

$$\Delta\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{\delta}{\delta} = 1$$

$$\Delta\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = 1 \longmapsto \frac{a}{\delta} \text{ et } \frac{b}{\delta} \text{ premiers entre eux}$$

Inversement, soit $d \in \mathbb{Z}^*$ un diviseur commun à a et b : $\frac{a}{d} = a' \in \mathbb{Z}^*$, $\frac{b}{d} = b' \in \mathbb{Z}^*$

Si $\Delta(a', b') = 1$, c'est que $\frac{\Delta(a, b)}{|d|} = 1$

$$d = \pm \Delta(a, b)$$

Ces 2 propriétés réciproques l'une de l'autre forment un critère de PGCD :

Parmi tous les diviseurs communs de a et b, le PGCD est celui qui vérifie : "Les quotients, entiers de a et b par ce diviseur, sont premiers entre eux

3°/ $\Delta(a, b) = 1$ et $\Delta(a, c) = 1$

a est donc premier avec b et c par hypothèse.

$\exists (u_0, v_0) \in \mathbb{Z}^2 \ / \quad a u_0 + b v_0 = 1$

$$a c u_0 + b c v_0 = c$$

Tout diviseur d commun à a et bc divise $a c u_0$, $b c v_0$, donc leur somme, donc c (et inversement)

Or, $\Delta(a, c) = 1 \vdash d = \pm 1$ voir autre démonstration cf cah 007

$\Delta(a, bc) = 1$

$$\Delta(a, b) = 1 \text{ et } \Delta(a, c) = 1 \vdash \Delta(a, bc) = 1 \qquad (3)$$

a, premier avec b et c, est premier avec le produit bc.

4°/ Théorème de Gauss.

hyp. $\begin{cases} a \mid bc \quad , \quad a \in \mathbb{Z}^* \ , (b, c) \in \mathbb{Z}^{*2} \\ \Delta(a, c) = 1 \end{cases}$

$\exists (u_0, v_0) \in \mathbb{Z}^2 \ / \quad a u_0 + c v_0 = 1$

$$b a u_0 + b c v_0 = b$$

a divisant $b a u_0$ et $b c v_0$, divise leur somme, donc divise b

Remarque : conséquence du théorème de Gauss

$\left.\begin{matrix} \Delta(a, b) = 1 \\ a \mid c \text{ et } b \mid c \end{matrix}\right\} \vdash ab \mid c$

a divisant $b.c$, et premier avec c, divise alors nécessairement b. (4)

plication

Résoudre en nombres entiers, l'équation :

$$6x - 7y = 1 \quad , \quad (x,y) \in \mathbb{Z}^2$$

6 et 7 sont premiers entre eux. L'égalité de Bezout est vérifiée pour un couple au moins (x,y)

ex : $x = -1$, $y = -1$

$$\begin{cases} 6x - 7y = 1 \\ 6(-1) - 7(-1) = 1 \end{cases}$$

$$6(x+1) - 7(y+1) = 0$$

$$6(x+1) = 7(y+1)$$

6 divise le 1er membre (car $x+1 \in \mathbb{Z}$). Donc 6 divise le 2e membre. Or, 6 est premier avec 7, donc (théorème de Gauss) 6 divise $y+1$.

$$y+1 = 6q \quad , \quad q \in \mathbb{Z}$$

De $6(x+1) = 7(y+1)$ on tire :

$$\cancel{6}(x+1) = 7.\cancel{6}q$$

$$x+1 = 7q$$

$$\begin{cases} x = 7q - 1 & q \in \mathbb{Z} \\ y = 6q - 1 \end{cases}$$

$x \in \{ \dots, -15, -8, -1, 6, 13, 20, \dots \}$

$y \in \{ \dots, -13, -7, -1, 5, 11, 17, \dots \}$

22.10

Recherche pratique de $\Delta(a, b)$

$a \in \mathbb{N}^*$, $b \in \mathbb{N}^*$ (cela n'enlève rien à la généralité de la méthode). $(a > b)$

Sinon, on opère avec $|a|$ et $|b|$.

1°/ $a = bq$, tout diviseur de b divise a.

$\Delta(a, b) = b$

2°/ $a = bq + r$ $\quad 0 \leq r < b$

Or, $\Delta(a, b) = \Delta(b, r)$ car, si :

α) tout d qui divise a et b divise a, bq, $a - bq$, donc r ; donc b et r.

β) tout d' qui divise b et r divise bq et r, a ; donc a et b.

γ) Les éléments les plus grands des 2 listes de diviseurs communs (listes identiques) coïncident.

On reprend le couple (b, r) et on fait une nouvelle division : $b = rq_1 + r_1$, $0 < r_1 < r$.

$\Delta(b, r) = \Delta(r, r_1)$

$$r = r_1 q_2 + r_2 \ , \quad 0 < r_2 < r_1$$

- - - - - - - - - - - - - - - - - - -

$$r_{n-2} = r_{n-1} q_n + \boxed{r_n} \ , \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + 0 .$$

Nécessairement, l'algorithme (succession d'opérations réitérées) se termine car les restes trouvés, entiers naturels, sont de plus en plus petits.

Il existe un dernier reste non nul. La dernière ligne montre : $\Delta(r_{n-1}, r_n) = r_n$

Or, $\Delta(r_{n-1}, r_n) = \Delta(r_{n-2}, r_{n-1}) = \dots$

$$= \Delta(r_1, r_2)$$

$$= \Delta(r, r_1) = \Delta(b, r)$$

$$= \Delta(a, b)$$

$$\boxed{\Delta(a, b) = \underbrace{\Delta(b, r)}_{r_n}}$$

Exemple

$a = 2375$, $b = 75$

$2375 = 75 \times 31 + 50$ $\qquad$ $50 < 75$

$75 = 50 \times 1 + 25$ $\qquad$ $25 < 50$

50 ~~25~~ $= 25 \times 2 + 0$

$r_n = 25$ $\qquad$ $\Delta(2375, 75) = 25$

Application

Résoudre dans $\mathbb{Z}^2$ $\quad$ $437x - 241y = 1$

$437 = 241 \times 1 + 196$

$241 = 196 \times 1 + 45$

$196 = 45 \times 4 + 16$

$45 = 16 \times 2 + 13$

$16 = 13 \times 1 + 3$

$13 = 3 \times 4 + 1$

$3 = 1 \times 3 + 0$

$\Delta(437, 241) = 1$

437 et 241 sont premiers entre eux.

On exprime les restes successifs uniquement à l'aide

de 437 et de 241.

$196 = 437 - 241$

$45 = 241 - 196 = 241 - (437 - 241)$

$45 = 2 . 241 - 437$

$16 = (437 - 241) - 8 \times 241 + 4 . 437$

$16 = 5 . 437 - 9 . 241$

$13 = 2 . 241 - 437 - 2 (5 . 437 - 9 . 241)$

$13 = 20 . 241 - 11 \times 437$

$3 = 5 . 437 - 9 . 241 - 20 . 241 + 11 . 437$

$3 = 16 . 437 - 29 . 241$

$1 = 20 . 241 - 11 . 437 - 4 (16 . 437 - 29 . 24$

$1 = -75 . 437 + 136 . 241$

$\exists (x_0, y_0) = (-75, -136)$

Alors :

$$\begin{cases} 437x - 241y = 1 & (1) \\ 437(-75) - 241(-136) = 0 \end{cases}$$

$$437(x + 75) = 241(y + 136) \quad (2)$$

Théorème de Gauss : $y + 136 = 437k$

$\forall k \in \mathbb{Z}$. On remplace dans (2) :

$x + 75 = 241k$

$$\begin{cases} x = 241k - 75 \\ y = 437k - 136 \end{cases} \quad \forall k \in \mathbb{Z}$$

$$\begin{cases} x \equiv -75\ [241] \\ y \equiv -136\ [437] \end{cases}$$

5.121

Diviseur commun à plusieurs entiers relatifs.

1°/ $\{a_1, a_2, a_3, \dots, a_k\}$ $(a_i)_{i\in[1,k]\cap\mathbb{N}} \neq 0$

$(a_1) = a_1\mathbb{Z}$ ou $(a_1) = -a_1\mathbb{Z}$

- - - - - - - - - - - - -

$(a_k) = a_k\mathbb{Z}$ ou $(a_k) = -a_k\mathbb{Z}$

$$A = (a_1) + (a_2) + \dots + (a_k) = \{x \in \mathbb{Z},\ \exists\, u_1, \dots, u_k \in \mathbb{Z} \ / \ x = a_1u_1 + \dots + a_ku_k\}$$

A est un idéal de $\mathbb{Z}$

α) $A \neq \emptyset$ $(\exists\, a_1 \in A)$

β) $(A, +)$ sous-groupe de $\mathbb{Z}$

γ) $\forall x \in A,\ \forall y \in \mathbb{Z},\ x \times y \in A$

$A \neq \{0\}$, sinon, c'est qu'on se serait donné tous les a_i nuls. $\exists!\ \delta > 0$, δ minimum et $\delta \in A$

Alors : $A = \delta\mathbb{Z}$

* $a_i \in A \vdash \exists q \in \mathbb{Z} \ / \ a_i = \delta q$

δ divise tous les a_i : $\delta \mid a_i$

* $\delta \in A \vdash \underset{\exists (v_1, \dots, v_k) \in \mathbb{Z}^k}{\delta = a_1 v_1 + a_2 v_2 + \dots + a_k v_k}$

$\forall d \in \mathbb{Z} \;/\; d \mid a_i \,,\; \forall i \in [1, k] \cap \mathbb{N}$, divise δ

Donc $\delta = PGCD(a_1, a_2, \dots, a_k)$

Remarque

Si $\delta = 1$, $\exists (u_1, u_2, \dots, u_k) \in \mathbb{Z}$

$1 = a_1 u_1 + \dots + a_k u_k$

Les a_i sont dits "premiers entre eux dans leur ensemble"

3.11 6 PPCM de 2 entiers relatifs non nuls a et b

$$(a) = \{x, x \in \mathbb{Z} ; \exists k \in \mathbb{Z} : x = ka\} = a\mathbb{Z}$$
$$(b) = \{x, x \in \mathbb{Z} / \exists k \in \mathbb{Z} : x = kb\} = b\mathbb{Z}$$

$\mathcal{I} = (a) \cap (b)$ = idéal ?

* $\mathcal{I} = (a) \cap (b)$ est-il un sous-groupe de $\mathbb{Z}$

En effet, $\mathcal{I} \neq \emptyset$: voir $0 = 0.\underline{a} = 0.\underline{b}$

$ab = b.\underline{a} = a.\underline{b}$

Et : $\forall x \in \mathcal{I}$, $\forall y \in \mathcal{I}$, $x + (-y) \in \mathcal{I}$?

$x \in \mathcal{I} \longmapsto x = ka = k'b \quad , (k, k') \in \mathbb{Z}^2$

$y \in \mathcal{I} \longmapsto y = qa = q'b \quad , (q, q') \in \mathbb{Z}^2$

$x - y = \underbrace{(k-q)}_{\in \mathbb{Z}} a = \underbrace{(k'-q')}_{\in \mathbb{Z}} b$

$x - y = Qa = Q'b \quad , (Q, Q') \in \mathbb{Z}^2$

$\underline{x - y \in \mathcal{I}}$

* On a vu que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$, donc est un idéal de $\mathbb{Z}$. Ici, c'est le cas

$$I = \mu \mathbb{Z} = (\mu)$$

μ étant l'entier naturel le plus petit de I.

μ = PPCM de a et b , $\mu > 0$

ex : $a = 45$ et $b = 10$

$$\mu = 90 = \underbrace{2}_{k} \times 45 = \underbrace{9}_{k'} \times 10$$

Propriétés du PPCM

1°/

$\mu = M(a, b) = \text{PPCM de } (a, b) = a \vee b = a \vee b$

$\mu' = M(ka, kb)$, $k \in \mathbb{Z}$

$\forall m' \in (\mu')$, $m' = kap = kbq$ $\quad (p, q) \in \mathbb{Z}^2$

$m' = kpa = kqb \in (\mu)$

$m' = h\mu$, $h \in \mathbb{Z}$

Revenons à :

$$m' = k\underbrace{(p\ a)}_{h_1 \mu} = k\underbrace{(q\ b)}_{h_1 \mu}$$

$m' = k . h_1 . \mu$

$m' = h_1 \underbrace{(k.\mu)}$

m' est un multiple de $k\mu$.

$m' \in (k\mu)$ donc $\underline{(\mu') \subset (k\mu)}$

Inversement, soit $m'' \in (k\mu)$

$m'' = k\ (k\mu) = k\ (h\mu)$

$m'' = k\,(h\mu)$

$m'' = k\ .\ pa\ = k\ .\ qb$

$m'' = p\ (ka) = q\ (kb)\ \vdash\ m'' =$ multiple commun à ka et kb. Donc $m'' \in (\mu')$

$\underline{(k\mu) \subset (\mu')}$

$(\mu') = (k\mu) \vdash$ $\boxed{\mu' = |k|\,\mu}$

3°/ Conséquence.

$\mu = M(a, b)$

$a = d\,a'$, $d \in \mathbb{Z}$

$b = d\,b'$ $\quad d =$ diviseur commun à a et b.

$\mu' = M(a', b')$

$|d|\,\mu' = M(\underbrace{d\,a'}_{a}, \underbrace{d\,b'}_{b})$

$\mu = |d|\,\mu'$ $\qquad \mu' = \dfrac{\mu}{|d|}$

$$M\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{M(a,b)}{|d|}$$

3°/ Une relation entre a, b, δ et μ.

$$\begin{cases} \Delta(ka, kb) = |k| \, \Delta(a,b) \quad (\text{rappel}) & (1) \\ M(k a, kb) = |k| \, M(a,b) & (2) \end{cases}$$

α) $|k| = M(a,b) = \mu$ dans la 1re égalité ($k = M$

(1) devient : $\mu . \delta = \Delta(\mu a, \mu b)$

$\mu a = a \mu = a \cdot M(a,b) = M(a^2, ab)$

$\mu b = b \mu = b . M(a,b) = M(ab, b^2)$

(ab) divise donc $\Delta(\mu a, \mu b)$ donc $\mu\delta$

ab divise $\mu\delta$

β) $|k| = \Delta(a,b) = \delta = k$

(2) devient : $\delta\mu = M(a\delta, b\delta)$

$a\delta = a\,\Delta(a,b) = \Delta(a^2, ab)$

$b\delta = b\,\Delta(a,b) = \Delta(ab, b^2)$

(a,b) est donc multiple de $\mu\delta$

Résumé : $a\,b \mid \mu\,\delta$

$\mu\,\delta \mid a\,b$

Donc $\mu\,\delta = |a\,b|$

$$\boxed{\mu\,\delta = |a\,b|}$$

<u>Remarque 1</u> : La relation $\mid$ est relation d'ordre dans $\mathbb{N}$, mais pas dans $\mathbb{Z}$.

<u>Remarque 2</u> : Si $a > 0$ et $b < 0$, $b = -b_1$ avec $b_1 > 0$. $|a\,b| = a\,b_1$

On se place dans le cas où a et b sont tous deux positifs $|a\,b| = a\,b_1 = \mu\,\delta$

(même μ et même δ pour les couples (a, b) et (a, b_1))

$a > 0$, $b > 0$

$$\begin{cases} a = \delta\,a' \\ b = \delta\,b' \end{cases} \quad \text{et} \quad \Delta(a', b') = 1$$

La relation $a\,b = \mu\,\delta$ devient

$$\delta\,a' . \delta\,b' = \mu\,\delta$$

$$\boxed{\delta\,a'\,b' = \mu}$$

or $\delta a' = a$ $\vdash$ $\boxed{\mu = a\,b'}$

et $\delta b' = b$ $\vdash$ $\boxed{\mu = a'\,b}$

$$\mu \delta = a b$$
si $ab > 0$

$$\mu = \delta a' b' = a b' = b a'$$
$$\Delta(a', b') = 1$$

plication : exercices.

1) $\begin{cases} M(a, b) = 60 \\ a = 12 \end{cases}$

trouver b

α) Supposons $b > 0$.

$60 . \delta = 12 . b$

$5 \delta = b$ → b = multiple de 5
et b divise 60.

$b = 5, 10, 15, 20, 30$, ou 60

Il existe 6 solutions.

β) Supposons $b < 0$.

$b = -5, -10, -15, -20, -30$, ou -60

4.11 2°/ 2ᵉ exemple.

$$\begin{cases} \delta = 36 \ ; \ \mu = 756 \\ \delta = \Delta(a, b) \ ; \ \mu = M(a, b) \end{cases}$$

Trouver (a, b) ?

Posons $|a| = \alpha$; $|b| = \beta$

$\alpha\beta = \mu\,\delta$

$\alpha\beta = 756 \times 36$

$\left.\begin{array}{l} \alpha = \delta\,\alpha' \\ \beta = \delta\,\beta' \end{array}\right\}$ avec $\Delta(\alpha', \beta')\ 1$

$\delta^2 \alpha'\beta' = 756 \times 36$ $\quad (\alpha', \beta') \in \mathbb{N}^2$

$756 = 36 \times 21$ (énoncé favorable)

Donc $\quad 36 \times 36 \times \alpha'\beta' = 36 \times$ ~~75~~ 36×21

$$\begin{cases} \alpha'\beta' = 21 \\ \Delta(\alpha', \beta') = 1 \end{cases}$$

α' et β' sont des diviseurs de 21.

La liste en est $(>)$: $\underline{21}$; $\underline{\underline{7}}$; $\underline{\underline{3}}$; $\underline{1}$

$\alpha' = 21$ et $\beta' = 1$

ou $\alpha' = 7$ et $\beta' = 3$

Si on demande des couples (α', β'), il y en a 4.

Sinon, il y a deux paires.

$$\begin{cases} \alpha = \delta\alpha' = 36 \times 21 \\ \beta = \delta\beta' = 36 \times 1 \end{cases}$$

$$\begin{cases} \alpha = 36 \times 7 \\ \beta = 36 \times 3 \end{cases}$$ vérification : $36.7.36.3 = 756.3$

$\exists$ 4 couples (α, β)

$\exists$ 16 couples (a, b) : signes associés $\begin{cases} + + \\ - - \\ + - \\ - + \end{cases}$

3°/ On donne $d = \mu - \delta = 18$ (1)

$\mu\delta = \alpha\beta = |a| \times |b|$

$\mu\delta = \alpha\beta = \delta\alpha' . \delta\beta'$

$\mu = \delta\alpha'\beta'$

(1) : $d = \delta\alpha'\beta' - 1\delta$

$18 = \underbrace{\delta}_{\in \mathbb{N}}\underbrace{(\alpha'\beta' - 1)}_{\in \mathbb{N}}$

$\Delta(\alpha', \beta') = 1$

δ est un diviseur positif de 18 :

18, 9, 6, 3, 2, 1

donc

$\alpha'\beta' - 1 = 1$ ou 2 ou 3 ou 6 ou 9 ou 18

$$\begin{cases} \alpha'\beta' = 2, 3, 4, 7, 10, \text{ ou } 19 \\ \Delta(\alpha', \beta') = 1; \overset{\alpha'\beta'=2}{\vdash} \alpha' = 1 \text{ et } \beta' = 2 \end{cases}$$

(ou inversement)

$\alpha'\beta' = 2 \vdash \{\alpha', \beta'\} = \{1, 2\}$

$\alpha'\beta' = 3 \vdash \{\alpha', \beta'\} = \{1, 3\}$

$\alpha'\beta' = 4 \vdash \{\alpha', \beta'\} = \{1, 4\}$

$\alpha'\beta' = 7 \vdash \{\alpha', \beta'\} = \{1, 7\}$

$\alpha'\beta' = 10 \vdash \{\alpha', \beta'\} = \{1, 10\}$ ou $\{2, 5\}$

$\alpha'\beta' = 19 \vdash \{\alpha', \beta'\} = \{1, 19\}$

$\{\alpha, \beta\} = \{18, 36\}$ car $\delta = 18$

$\{\alpha, \beta\} = \{9, \overset{27}{\cancel{36}}\}$ car $\delta = 9$

$\{\alpha, \beta\} = \{6, 24\}$ car $\delta = 6$

etc ...

22.11 7 Nombres premiers

p premier a 4 diviseurs : $\{1, -1, p, -p\}$

$1 \neq$ nombre premier

2, 3, 7, 11 sont premiers.

$16 \neq$ nombre premier

Première propriété

"Tout nombre non premier ($\neq 1$) admet au moins un diviseur premier : c'est le plus petit des diviseurs du nombre donné, du moins dans $\mathbb{N} - \{1\}$

ex : 42 a pour diviseurs :

42, -42, 21, -21, 7, -7, 6, -6, 3, -3, 1, -1, 14, (2), -2.

143 a pour diviseurs : 143, 13, (11), 1, -1, -11, -13, -1…

$n = d . d'$

$d \leqslant d'$

Ex : $49 = 7 \times 7$ ou : $143 = 11 \times 13$

$d \leq d'$ (d = le diviseur premier signalé ci-dessus.)

$d^2 \leqslant dd'$

$d^2 \leqslant n$

Donc n non premier différent de 1 admet $d \neq 1$, diviseur de n
et d premier tel que $d^2 \leqslant n$.

C'est la contraposée de cette propriété qui est utile pratiquement :
Pour chercher si un nombre n est, ou non, premier, on effectue les divisions successives de n par les entiers naturels premiers à partir du plus petit et dans l'ordre croissant. De 2 choses l'une :
* ou bien une division donne un reste nul ; n n'est pas premier
* ou bien aucune des divisions par les d / $d^2 \leqslant n$ n'a donné de reste nul. On conclut que n est premier.

Le critère d'arrêt dans la liste des diviseurs essayés est $d^2 > n$ d est le diviseur essayé.

Il y en a un plus simple :

pour 491

exemple : $491 = \textcircled{19} \times 25 + 16$

$491 = \textcircled{23} \times 21 + 8$

$19^2 = 361$; $23^2 = 529$

Au moment où le quotient devient inférieur au diviseur essayé, alors le carré du diviseur essayé dépasse 491 : alors on peut s'arrêter : 491 est premier.

Plus généralement : $\begin{cases} n = \textcircled{p}\, q + r & , \quad r < p \\ \text{et } q < p \end{cases}$

donc $pq < p^2$

ou encore $q < p \vdash q + 1 \leq p$

$$pq + \textcircled{r} < pq + \textcircled{p} \leq p^2$$

car $r < p$

$$\overbrace{pq + r}^{n} < p^2$$

$$p^2 > n$$

$\underbrace{q < p}_{} \vdash p^2 > n$

critère suffisant d'arrêt

…liste des nombres premiers est illimitée

Si $\exists p$ premier, on arrive à trouver un p' premier, $p' > p$; donc l'ensemble des nombres premiers n'est pas majoré.

Soit $n = p! + 1$

* ou bien n tombe premier et $\exists n > p$, n premier.
* ou bien $n \neq$ nombre premier et alors n admet au moins 1 diviseur p' premier ; mais ce n'est aucun des facteurs premiers composant $p!$ (voir reste égal à 1)

$n = 2, 3 \ldots (q) \ldots p + 1$

Donc $p' > p$ et p' premier

…nombres premiers et divisibilité (cf C7 60)

…dans $\mathbb{N}$)
…t p un nombre premier
… ne divise pas un
…tier a. Les seuls
…viseurs communs
…ssibles sont p et 1
…mme p ne divise pas
…, p et a sont
…miers entre eux.

① "p premier est "premier avec" tout ce qu'il ne divise pas"

* $19 | 38$ — 19 n'est pas premier avec 38
* 19 ne divise pas 37 } 19 premier avec 37, et avec 64.
  19 " " 64 }

② Deux nombres premiers différents (en valeurs absolues) sont premiers entre eux.

…équence de ①

Soit p_1 et p_2 premiers ; si $|p_1| \neq |p_2|$, alors

p_1 et p_2 sont premiers entre eux.

Remarque : 19 et −19 ont 19 pour PGCD
$\Delta(19, -19) \neq 1$

③ Tout diviseur p premier d'un produit a b c, divise nécessairement ou a, ou b, ou c.

* Soit p premier diviseur de a b
Il peut diviser a ; sinon, il est premier avec a et alors le ~~théor~~ théorème de Gauss s'applique : et p divise b.

* Soit p premier de a b c
p peut diviser a ou b ; sinon, il ne divise ni a, ni b ; il est donc premier avec les 2 ; donc premier avec a b (théorème du 21.10) ; puis (th. de Gauss), p divise c.

④ Tout diviseur p premier d'un produit a b c de nombres premiers a pour valeur absolue : |a| ou |b| ou |

...etour sur l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$

* $n = 0$ $\quad x \equiv y \ [0] \quad , (x,y) \in \mathbb{Z}^2$

$x = y + k.0 \vdash x = y$

$y = x \vdash \dot{x} = \{x\}$; l'ensemble $\mathbb{Z}/0\mathbb{Z}$ isomorphe à $\mathbb{Z}$, anneau.

* $n = 1$ $\quad x \equiv y \ [1]$

$x = y + k \ , k \in \mathbb{Z}$

$\exists! \dot{0} \ s/ \ x \in \dot{0} \ , y \in \dot{0}$

* $n \geqslant 2$

on cherche les éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles :

ex : $\dot{x}$ inversible ssi :

$\exists \dot{x}' \in \mathbb{Z}/n\mathbb{Z} \ / \ \dot{x} \times \dot{x}' = \dot{1}$

$\overline{xx'} = \dot{1}$

$xx' \equiv 1 \ [n]$

$xx' - 1 = kn \quad , k \in \mathbb{Z}$

$xx' - kn = 1$

donc $\quad \Delta(x, n) = 1$

donc les classes $\dot{x}$ de $\mathbb{Z}/n\mathbb{Z}$ qui seront inversibles seront celles vérifiant , $x \in \{0, 1, 2, \ldots, n-1\}$,

x premier avec n.

ex : si $n = 6$

$x = 0$, $\dot{0}$ non inversible.

$x = 1$ oui $\quad x = 3$ non $\quad x = 5$ ou[i]

$x = 2$ non $\quad x = 4$ non

$\dot{1}$ et $\dot{5}$ sont les seules classes inversibles de $\mathbb{Z}/6\mathbb{Z}$

Distinction entre les 2 cas :

n premier.

n non premier.

1°/ n premier.

Alors seule $\dot{0}$ vérifie

$0 = kn \quad k \in \mathbb{Z}$

$\dot{0} = \dot{n}$

Les autres classes vérifient $\Delta(x, n) = 1$

$\{\mathbb{Z}/n\mathbb{Z} - \{\dot{0}\}, \times\}$ = groupe.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ = corps commutatif.

2°/ n non premier

$\exists (p,q) \in \mathbb{Z}^2 \ / \ n = p.q \ , \ p \neq 1$ et $q \neq 1$.

$p \in \{1, 2, \dots, n-1\}$

$q \in \{1, 2, \dots, n-1\}$

$\Delta(n, p) = p \neq 1$

$\dot{p}$ non inversible

$\exists$ classe non inversible

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ n'est **pas** un corps

« $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier ».

25.11

Décomposition d'un entier en produit de facteurs premiers

$N' \in \mathbb{Z} \quad , \quad N = |N'|$

Si N est premier : N = N (premier)

Si N n'est pas premier, alors $\exists \, p_1$ premier diviseur de N :

$N = p_1 \, q_1$

Si q_1 est premier, la décomposition est terminée.

Si q_1 n'est pas premier, $\exists \, p_2$ premier diviseur de q_1

$q_1 = p_2 \, q_2$

$N = p_1 p_2 q_2$

etc ...

$\exists\ q_k \ \text{ / } = p_k$ premier, car $N > q_1 > q_2 > \dots > q_k$.

Donc :

$N = p_1 p_2 p_3 \dots p_k$ (k facteurs premiers.

$$N' = \varepsilon . p_1 \ p_2 \dots p_k$$ $\varepsilon = \pm 1$

Cette décomposition est unique.

Si $N = p_1 . p_2 \dots p_k = p_1' p_2' \dots p_m'$

Tout p_i figure dans le membre de droite.

Tout p_j' figure dans le membre de gauche.

Les décompositions coïncident.

Pratique : $N = p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_k^{\alpha_k}$

Application à la recherche des diviseurs et ~~et~~ des multiples d'un nombre

1. Les diviseurs (cf Encyclopédie tome 2 p 16)

$N = p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$N = dq \ / \ d \in \mathbb{N}, q \in \mathbb{N}$, pour commence

$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdots p_k^{\delta_k} \qquad 0 \leq \delta_i \leq \alpha_i$

Le nombre total de diviseurs s'obtient en cherchant combien on peut faire de produits de k facteurs en extrayant chacun des facteurs d'un ensemble de cardinal $(\alpha_1 + 1)$, pour le premier, $(\alpha_2 + 1)$, pour le second, ..., $(\alpha_k + 1)$, pour le dernier.

Liste des $(\alpha_1 + 1)$ exposants possibles pour p_1 :

$0, 1, 2, \ldots, \alpha_1$

Nombre de diviseurs de N^*

$n = \underbrace{2}(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$

pour symétriser.

Le nombre N' aura le même nombre de diviseurs (positifs ou négatifs) que N.

Bien sûr, dans $\mathbb{N}$, nous aurons un nombre total de diviseurs entiers naturels égal à :

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$$

2. Les multiples

$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$m = N \cdot q'$

$m = p_1^{\mu_1} \cdot p_2^{\mu_2} \cdots p_k^{\mu_k} \cdot q''$ $\qquad \mu_i \geqslant \alpha_i$

PGCD et PPCM de 2 entiers naturels décomposés en produits de facteurs premiers

$$\begin{cases} A = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \\ B = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m} \end{cases}$$

On s'est arrangé pour que les mêmes facteurs premi[ers] interviennent dans les 2 décompositions.

ex : $A = 2^3 . 7^2 \times 3^0 \times 11^0$

$B = 2^4 . 7 . 3 . 11^5$

D = diviseur commun à A et B :

$D = 2^{\delta_1} . 7^{\delta_2} . 3^{\delta_3} . 11^{\delta_4}$

$0 \leq \delta_1 \leq 3$

$0 \leq \delta_2 \leq 1$

$0 \leq \delta_3 \leq 0$

$0 \leq \delta_4 \leq 0$

$PGCD(A, B) = 2^3 . 7$

Un multiple M commun à A et B est tel que

$M = 2^{\mu_1} . 7^{\mu_2} . 3^{\mu_3} . 11^{\mu_4}$

$\mu_1 \geqslant 4 \qquad \mu_3 \geqslant 1$ donc $M(A, B) = 2^4 . 7^2 . 3^1 .$

$\mu_2 \geqslant 2 \qquad \mu_4 \geqslant 5$

8 Ensemble des Réels

Définition axiomatique de $\mathbb{R}$

1°/ $(\mathbb{R}, +, \times)$ = corps commutatif

2°/ $(\mathbb{R}, \leq)$ = ensemble totalement ordonné par la relation $\leq$.

compatibilité de + par $\leq$ * $\forall (x, y, z) \in \mathbb{R}^3$, $x \leq y \vdash x + z \leq y + z$

" de × par $\leq$ * $\forall\, 0 \leq z$, $x \leq y \longmapsto xz \leq yz$

3°/ Toute partie $P \subset \mathbb{R}$; $P \neq \emptyset$, P majorée, possède alors une borne supérieure dans $\mathbb{R}$.

Propriétés

1°/ Valeur absolue d'un réel x.

$$|x| = \text{Sup}(x, -x)$$

Donc $|x| = x$ si $x \geqslant 0$

$|x| = -x$ si $x \leqslant 0$

$$|xy| = |x| . |y|$$

$$|x + y| \leqslant |x| + |y|$$

$$\left| |x| - |y| \right| \leqslant |x + y|$$

2°/ (E, d) = espace métrique : c'est un ensemble munis d'une "distance".

$d : E \times E \longrightarrow \mathbb{R}^+$

$(x, y) \longmapsto d(x, y)$

3 propriétés
* $d(x, y) = 0 \longmapsto x = y$
* $d(x, y) = d(y, x)$
* $d(x, y) \leqslant d(x, z) + d(z, y)$

Ici, $E = \mathbb{R}$

$d(x, y)$? $x \in \mathbb{R}$, $y \in \mathbb{R}$. On convient de choisir $d(x, y) = |x - y|$, sous réserve de vérification :

$$d(x, y) = |x - y|$$

* $|x - y| = 0 \longmapsto x = y$
* $|x - y| = |y - x|$
* $|x - y| \leqslant |x - z| + |z - y|$?

En effet

$x - y = (x - z) + (z - y)$

$|(x - z) + (z - y)| \leq |x - z| + |z - y|$

troduction du corps $\mathbb{Q}$: c'est un sous-corps de $\mathbb{R}$

$\mathbb{Q} / \quad \mathbb{Z} \times \mathbb{Z}^*$

$a \in \mathbb{Z} \ ; \ b \in \mathbb{Z}^*$

$\underbrace{(a, b)}_{\text{fraction}} \in \mathbb{Z} \times \mathbb{Z}^*$

$x = (a, b)$ ~~$\in \mathbb{R}$~~ $/ \quad x \times b = a$

On crée ainsi de nouveaux nombres, non entiers relatifs qui jouiraient de la propriété ci-dessus.

Mais il existe plusieurs couples tels que (a, b) qui répondraient à la même définition ; c'est-à-dire :

$x \times b = a$

$x' \times b = a$

$x'' \times b = a$

On remarque, dans le cas où x, x', x'' sont entiers relatifs, que les couples qui les représentent vérifient $ab' = ba'$ avec 1er couple $= (a, b)$

2e couple $= (a', b')$

Alors on définie dans $\mathbb{Z} \times \mathbb{Z}^*$ une relation binaire :

$(a, b) \mathcal{R} (a', b') \mapsto ab' = ba'$

ex : $(a, b) = (4, 3)$

$(a', b') = (-20, -15)$

$4 \times (-15) = 3(-20)$

On montre que $\mathcal{R}$ est une relation d'équivalence. Donc il existe des classes d'équivalence. Chacune est appelée nombre rationnel

ex : $(4, 3) \mathcal{R} (-20, -15)$

$\exists$ nombre rationnel qu'on convient de nommer en utilisant les plus petites valeurs absolues de a et b

ex : ici $(4, 3)$, mieux $\frac{4}{3}$

$\Delta(4, 3) = 1$ tandis que $\Delta(-20, -15) = 5$

On dit que la fraction $\frac{4}{3}$ est irréductible

Borne supérieure et borne inférieure

Définition d'une borne supérieure B.S :

1°/ BS est un majorant

$\forall a, a \in P, \; a \leq BS$

2°/ BS est le plus petit des majorants

$\nexists m, m \in$ (Ens. des majorants) / $m < BS$

Une borne inférieure BI vérifie :

1°/ $\forall a \in P,\ BI \leqslant a$

2°/ $\exists\, m \in$ (Ens. des minorants) / $BI < m$.

P est dite bornée si P admet une BS et une BI.

Bien entendu, dans ce cas $BI \leqslant BS$ (voir $BI \leqslant a \leqslant BS$)

3.12 Caractérisation d'une borne supérieure.

a β b $\alpha = BS$

$\alpha = BS$ de P, $P \subset \mathbb{R}$

$\forall a \in P,\ a \leqslant \alpha$.

$\forall \beta,\ \beta \in \mathbb{R},\ \beta < \alpha,\ \exists\, b,\ b \in P \ /\ \beta < b \leqslant \alpha$

En d'autres termes

$\beta = \alpha - \varepsilon\ ,\ \varepsilon \in \mathbb{R}_+^*$

$\forall \varepsilon \in \mathbb{R}_+^*,\ \exists\, b,\ b \in P \ /\ \alpha - \varepsilon < b \leqslant \alpha$

Inversement : si un majorant de P possède la propriété ci-dessus, est-ce, à coup sûr, le plus petit majorant donc est-ce BS ?

Donc : $\forall a \in P,\ a \leqslant \alpha$

$\forall \varepsilon \in \mathbb{R}_+^*,\ \exists\, b \in P \ /\ \alpha - \varepsilon < b \leqslant \alpha$

S'il existait un autre majorant de P, et $\alpha' < \alpha$

alors

α' β α

ε

Il suffit de choisir un ε tel que $\varepsilon < \alpha -$

alors $\exists b \,/\, \alpha - \varepsilon < b \leq \alpha \quad b \in P$

$$\alpha' < \alpha - \varepsilon < b \leq \alpha$$

on aurait $\alpha' < b$ } incompatibilité.
et, α' majorant }

Donc $\nexists \alpha'$, $\alpha' < \alpha$ et α' majorant de P.

Donc $\alpha = BS$

La propriété ci-dessus constitue donc un critère de borne supérieure de P.

De même, critère de borne inférieure pour P.

1°/ $\forall a,\ a \in P,\ \beta \leq a\ ,\ \beta = BI$

2°/ $\forall \varepsilon \in \mathbb{R}_+^*,\ \exists b,\ b \in P \,/$

$$\beta \leq b < \beta + \varepsilon$$

$BI = \beta$ b $(\beta + \varepsilon)$ a

ε

Remarque :

BS, (ou BI) fait ou non partie de P, on ne le sait

pas à l'avance. Si oui, BS (resp. BI) est le plus grand élément de P (resp. le plus petit élément de P)

Intervalles de $\mathbb{R}$

1°/ Définition :

$[a, b]$; $(a, b) \in \mathbb{R}^2$

$[a, b] = \{x, x \in \mathbb{R} \ / \ a \leq x \leq b\}$

$[a, b[= \{x, x \in \mathbb{R} \ / \ a \leq x < b\}$

$[a, a] = \{a\}$

$[a, a[= \emptyset =]a, a] =]a, a[$

$[a, +\infty[= \{x, x \in \mathbb{R} \ / \ a \leq x\}$

$]-\infty, b] = \{x, x \in \mathbb{R} \ / \ x \leq b\}$

$]-\infty, +\infty[= \mathbb{R}$

On adjoint à $\mathbb{R}$ l'ensemble $\{-\infty ; +\infty\}$ qui n'est pas une ~~couple~~ paire de nombres, mais qui permet de former :

$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty ; +\infty\}$ avec $\mathbb{R} \cap \{-\infty, +\infty\} = \emptyset$

De plus, on ordonne $\overline{\mathbb{R}}$ ainsi :

1°/ $\forall (x, y) \in \mathbb{R}^2$, $x \leq y$ est la relation connue.

2°/ $\forall x \in \overline{\mathbb{R}}$, $x \leq +\infty$

3°/ $\forall x \in \overline{\mathbb{R}}$, $-\infty \leq x$

2°/ Propriété d'un intervalle I de $\mathbb{R}$, $I \neq \emptyset$.

$\forall (x,y) \in I^2$, $[x,y] \subset I$ $\quad x \leq y$ (= sans intérêt)

ex : $I =]a, +\infty[$

$a < x < y < +\infty$

$\forall r \in [x,y]$, alors $r \in I$

3°/ Inversement

-.12 Soit une partie P de $\mathbb{R}$, non vide, telle que, $\forall (x,y) \in P^2$, $x \leq y$, alors $[x,y] \subset P$, alors on va montrer que P est un intervalle.

1 → * supposons que P est bornée :

$\exists! \alpha = BS$, $\exists! \beta = BI$ de P.

On voit vite que $P \subset$ ~~$[\alpha, \beta]$~~ $[\beta, \alpha]$

Inversement, $\forall r \in \mathbb{R}$, $r \in]\beta, \alpha[$

$\forall r \in]\beta, \alpha[$, $\varepsilon = \alpha - r$, alors $\exists y \in P$, $r < y \leq \alpha$

$\varepsilon' = r - \beta$, alors $\exists x \in P$, $\beta \leq x < r$

Donc $\quad \beta \leq x < r < y \leq \alpha$

D'après l'hypothèse : $[x,y] \subset P \vdash \underline{r \in P}$

Donc $P = [\beta, \alpha]$ ou $]\beta, \alpha]$ ou $]\beta, \alpha[$ ou $[\beta, \alpha[$, P est un intervalle.

Remarques: Si $\beta = \alpha$, alors $P \neq \emptyset$ coïncide avec $\{\alpha\}$, donc $P = [\alpha, \alpha]$ et P = intervalle.
Dans le cas général : $\alpha \neq \beta$, l'hypothèse : P non vide, intervient quand on annonce : $\exists y \in P, r < y \leq \alpha$

2 → * Supposons que P est bornée supérieurement et non bornée inférieurement.
$\forall u \in P, \ u \leq \alpha$, donc $P \subset]-\infty, \alpha]$.
$\forall r \in]-\infty, \alpha[$

$\varepsilon = \alpha - r$, $\exists y \in P \ / \ r < y \leq \alpha$
$\exists x \in P \ / \ x < r$ (voir P non bornée inférieurement)
$-\infty < x < r < y \leq \alpha$
$r \in]x, y[\vdash r \in P$
$\forall r \in]-\infty, \alpha], r \in P$
Donc $P =]-\infty, \alpha[$ ou $]-\infty, \alpha]$.

3 $\longrightarrow$ * Si P admet $\beta = BI$ et <u>non</u> $\alpha = BS$, alors

$P \subset [\beta, +\infty[$

$\forall r \in]\beta, +\infty[$

β r $\mathbb{R}$

$\varepsilon = r - \beta$ $\exists x \in P$ / $\beta \leq x < r$

$\exists y \in P$ / $r < y$ (voir $\nexists \alpha = BS$)

$\beta \leq x < r < y < +\infty$

donc $r \in P$

$P = [\beta, +\infty[$ ou $]\beta, +\infty[$

4 $\longrightarrow$ * $\nexists \alpha = BS$; $\nexists \beta = BI$ pour la partie P.

$P \subset \mathbb{R}$

$\mathbb{R}$

$\forall r \in \mathbb{R} =]-\infty, +\infty[$

$\exists x < r$, $\exists y > r$

$-\infty < x < r < y < +\infty$

donc $r \in P$

donc <u>$P = \mathbb{R}$</u>

11.12

$\mathbb{R}$ est archimédien (propriété d'Archimède) $\forall a \in \mathbb{R}, \exists n \in \mathbb{N} / a < n$

$$\forall x \in \mathbb{R}_+^*, \forall y \in \mathbb{R}, \exists n \in \mathbb{N} / \quad y < nx$$

Conséquence.

$$P = \{ p, p \in \mathbb{N} / \quad p > x, \ x \in \mathbb{R} \text{ et } x \text{ donné} \}$$

* $P \neq \emptyset$ ($\mathbb{R}$ est archimédien)
* P est minorée par x.
* $\exists$ BI pour P, mais il existe plus petit élément.

Donc BI = ce plus petit élément ; soit n'.

$$\begin{cases} n' > x \\ \nexists p, p \in P ; p < n' \end{cases}$$

$\exists (n'-1) \in \mathbb{N}$, $n'-1 \notin P$

$\underbrace{(n'-1)}_{n} \leqslant x$

$\exists n \leqslant x$ tel que $\boxed{n \leqslant x < n+1}$

ex : $x = 5{,}6$ alors $n = 5$

$x = 5$, alors $n = 5$

Remarque : Il se peut qu'on introduise un jour, dans

que j'aime à faire apprendre un nombre utile aux sages
3,1415926535

un problème, un entier m tel que : $\underbrace{m}_{l-1} < x \leq \underbrace{m+1}_{l}$

Par ex : $x = 5,6$ $\quad 5 < 5,6 < 6$

$x = 5$ $\quad 4 < 5 \leq 5$

Q (ens. des rationnels) est dense dans R

1°/ $\forall (a,b) \in \mathbb{R}^2,\ a<b,\ \exists\ \frac{p}{n} \in \mathbb{Q}$

tel que $a < \frac{p}{n} < b$

2°/ $\exists$ infinité de rationnels analogues à $\frac{p}{n}$.

a $\exists \frac{p'}{n'} \in \mathbb{Q}$ b
$q \in \mathbb{Q}$ ↑ rationnels $\mathbb{R}$

Valeur approchée à 10^{-n} près d'un réel.

$\underbrace{6,45}_{\text{v.a. par défaut de } 6,453} < 6,453 < \underbrace{6,46}_{\text{v.a. par excès de } 6,453}$

$\underbrace{3,1415926}_{\alpha} < \pi < \overbrace{3,1415927}^{\beta}$

$\beta - \alpha = 10^{-7}$

suites adjacentes 1°/ 1 croissante et 1 décroissante

2°/

3°/ $\beta - \alpha \to 0$

Revenons à $x = 6,453$

$$x \cdot 10^3 = 6453$$

$$x \cdot 10^2 = 645,3 \qquad 645 \leqslant 645,3 < 646$$

$$p_n \leqslant x \cdot 10^2 < p_n + 1$$

$$\underbrace{p_n \cdot 10^{-2}} \leqslant x < (p_n + 1) 10^{-2}$$

valeur approchée par défaut de x à 10^{-2} près.

Valeurs approchées par défaut et par excès à 10^{-k} près ($k \in \mathbb{N}$) (cf C1 172).

$\forall x \in \mathbb{R}$, $\forall k \geqslant 0$, $\exists\, p_k$ unique tel que

$$p_k \leqslant 10^k x < p_k + 1$$

p_k est la partie entière de $10^k x$.

On a :

$$p_k \cdot 10^{-k} \leqslant x < (p_k + 1) 10^{-k}$$

$a_k = p_k \cdot 10^{-k}$ est appelé valeur approchée par défaut à 10^{-k} près de x.

$b_k = (p_k + 1) 10^{-k}$ est appelé valeur approchée par excès à 10^{-k} près de x.

Nombres complexes.

Rappel

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \quad (a,b,c,d) \in \mathbb{R}^4$$

$\mathcal{M}_2 = \{$ensemble des A , $\forall (a,b,c,d) \in \mathbb{R}^4\}$

$(\mathcal{M}_2, +, \times)$ = anneau unitaire non commutatif.

On rappelle l'isomorphisme d'anneaux entre $(\mathcal{L}(E), +, \circ)$ et $(\mathcal{M}_2, +, \times)$, $\mathcal{L}(E)$ = ensemble des endomorphismes de E (dimension 2).

Etude de l'ensemble $\mathbb{C}$ des matrices de la forme $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

$$z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

1°/ $(\mathbb{C}, +)$ = groupe commutatif

$\forall z_1 \in \mathbb{C}, \forall z_2 \in \mathbb{C}, \quad z_1 + (-z_2) \in \mathbb{C}$

En effet :

$$z_1 + (-z_2) = \begin{bmatrix} a_1 - a_2 & -b_1 + b_2 \\ b_1 - b_2 & a_1 - a_2 \end{bmatrix} = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \in \mathbb{C}$$

$\mathbb{C} \neq \emptyset$, exemple $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$2° \left(\mathbb{C}^* = \mathbb{C} - \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \times \right) = \text{groupe commutatif}$$

$$z_1 \times z_2 = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} = \underbrace{\begin{bmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - a_2b_1 \\ a_2b_1 + a_1b_2 & -b_1b_2 + a_1a_2 \end{bmatrix}}_{\in \mathbb{C}}$$

Il est suffisant maintenant de montrer l'existence de $z^{-1} \in \mathbb{C}^*, \forall z \in \mathbb{C}^*$

$$z \times z^{-1} = z^{-1} \times z = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

On trouve z^{-1} : $z^{-1} = \dfrac{1}{a^2+b^2} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$

$$z^{-1} = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \in \mathbb{C}$$

2.12 De plus $\times$ est commutative dans $\mathbb{C}$.

$$z_1 \times z_2 = z_2 \times z_1 = \begin{bmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - a_2b_1 \\ a_2b_1 + a_1b_2 & a_1a_2 - b_1b_2 \end{bmatrix}$$

L'échange des indices 1 et 2 conserve la matrice-produit.

$(\mathbb{C}^*, \times)$ = groupe commutatif

En résumé : $(\mathbb{C}, +, \times)$ = corps commutatif

De plus $\mathcal{C}$ est un sous-anneau commutatif, unitaire de l'anneau $\mathcal{M}_2$. De plus $\mathbb{C}$ étant un corps est un anneau intègre :

$$z_1 \times z_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \longmapsto z_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ ou } z_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

On appelle $\mathbb{C}$ le corps des nombres complexes.

$\mathbb{R}$ est un sous-corps de $\mathbb{C}$.

Soit $S \subset \mathbb{C}$ / S est l'ensemble des matrices du type $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, dites 1°/ matrices diagonales.
2°/ matrices scalaires.

Soit φ une application de $\mathbb{R}$ sur S

$$\varphi : \mathbb{R} \longrightarrow S$$

$$a \longmapsto \varphi(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

$$a' \longmapsto \varphi(a') = \begin{bmatrix} a' & 0 \\ 0 & a' \end{bmatrix}$$

$$a + a' \longmapsto \varphi(a + a') = \begin{bmatrix} a+a' & 0 \\ 0 & a+a' \end{bmatrix}$$

donc $\varphi(a + a') = \varphi(a) \boxplus \varphi(a')$

φ étant visiblement bijective, φ est un isomorphisme entre $(\mathbb{R}, +)$ et $(S, +)$. De plus, c'est un

isomorphisme de groupe.

De plus $a \longmapsto \varphi(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$

$a' \longmapsto \varphi(a') = \begin{bmatrix} a' & 0 \\ 0 & a' \end{bmatrix}$

$a \times a' \longmapsto \varphi(a \times a') = \begin{bmatrix} aa' & 0 \\ 0 & aa' \end{bmatrix}$

$\varphi(a) \times \varphi(a') = \begin{bmatrix} aa' & 0 \\ 0 & aa' \end{bmatrix}$

donc $\varphi(aa') = \varphi(a) \times \varphi(a')$

φ est encore un isomorphisme entre les 2 groupes multiplicatifs $\mathbb{R}^*$ et S^*

φ est un isomorphisme de corps

$\varphi : \mathbb{R} \longrightarrow S$

On convient de dire que $S = \mathbb{R}$ (on identifie $\mathbb{R}$ à S)

$\mapsto \varphi = Id$

S = corps ; $S \subset \mathbb{C}$ (corps)

$\mathbb{R}$ est un sous-corps de $\mathbb{C}$

$\mathbb{C}$ est un espace vectoriel sur $\mathbb{R}$

* $\forall \lambda \in \mathbb{R}$, $\forall z \in \mathbb{C}$

$\lambda . z = z'$

En effet $\lambda \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} \lambda a & -\lambda b \\ \lambda b & \lambda a \end{bmatrix} = z'$

On peut aussi poser $\lambda = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$, $z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, on fait le produit de 2 matrices, on trouve z'.

* $(\mathbb{C}, +)$ = groupe commutatif

De plus $\forall \lambda \in \mathbb{R}, \forall (z, z') \in \mathbb{C}^2, \lambda(z + z') = \lambda z' + \lambda z$

$\forall (\lambda, \mu) \in \mathbb{R}^2, \forall z \in \mathbb{C}^2, (\lambda + \mu) z = \lambda z + \mu z$

$\forall (\lambda, \mu) \in \mathbb{R}^2, \forall z \in \mathbb{C}, \lambda \mu z = \lambda(\mu z)$

$\forall z \in \mathbb{C}, \ 1 . z = z$

Recherche d'une base

$$z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = a \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{\text{c'est le réel } 1} + b \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{i}$$

i est un nombre complexe.

La partie $\{1, i\}$ est donc génératrice de $\mathbb{C}$ puisque

$\forall z \in \mathbb{C}, \ z = a . 1 + b . i \qquad (a, b) \in \mathbb{R}^2$

Est-elle libre ?

Oui, si et seulement si

$$\alpha \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \beta \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \vdash \alpha = \beta = 0$$

Or

$$\begin{cases} \alpha . 1 + \beta . 0 = 0 \vdash \alpha = 0 \\ \alpha . 0 + \beta . 1 = 0 \vdash \beta = 0 \\ \alpha . 0 + \beta (-1) = 0 \vdash \beta = 0 \\ \alpha . 1 + \beta . 0 = 0 \vdash \alpha = 0 \end{cases} \qquad \alpha = \beta = 0, \text{ oui.}$$

$(1, i)$ = base de $\mathbb{C}$

Conséquence :

$\forall z \in \mathbb{C}, \ \exists ! (a, b) \in \mathbb{R}^2 \ / \ z = a + bi$

Conséquence 2 : $z = z' \longmapsto a = a'$ et $b = b'$

puisque $z = a + bi$

$z' = a' + b'i$ et $\exists ! (a, b) \in \mathbb{R}^2$

$\alpha + \beta i = 0 \vdash \alpha = \beta = 0$

Carré de i

$$i^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \underbrace{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}_{\in S = \mathbb{R}}$$

$$\boxed{i^2 = -1}$$

$x^2 = -1 \vdash x = -i$ ou $x = i$

13.12

Application : $x^2 + x + 1 = 0$ à résoudre dans $\mathbb{C}$

$$x^2 + x + 1 = 0$$

$$\left(x + \frac{1}{2}\right)^2 - \frac{1}{4} + 1 = 0$$

$$\left(x + \frac{1}{2}\right)^2 = -\frac{3}{4} = \frac{3}{4}(-1) = \frac{3}{4}i^2$$

$$\left(x + \frac{1}{2}\right)^2 - \frac{3}{4}i^2 = 0$$

d'où $\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\left(x + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = 0$

$$\begin{cases} x' = -\frac{1}{2} - i\frac{\sqrt{3}}{2} \\ x'' = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \end{cases}$$

$$x = \frac{-1 \pm i\sqrt{3}}{2}$$

2- exemple

$$x^2 - x + 2 = 0$$

$$\left(x - \frac{1}{2}\right)^2 - \frac{1}{4} + \frac{8}{4} = 0$$

$$\left(x - \frac{1}{2}\right)^2 = -\frac{7}{4} = \frac{7}{4} i^2$$

$$\left(x - \frac{1}{2} + \frac{\sqrt{7}}{2} i\right)\left(x - \frac{1}{2} - \frac{\sqrt{7}}{2} i\right) = 0$$

$$x = \frac{1 \pm i\sqrt{7}}{2}$$

les 4 opérations

1°/ $z = a + bi$; $z' = a' + b'i$

$z + z' = (a + a') + (b + b')i$

2°/ $z - z' = (a - a') + (b - b')i$

3°/ $z \times z' = zz'$

$zz' = (a + bi)(a' + b'i)$

$= (aa' - bb') + (ab' + ba')i$

4°/

$$\frac{1}{z'} = \frac{1}{a'+b'i} = \frac{a'-b'i}{a'^2+b'^2} \quad , \text{ si } z' \neq 0 \vdash a' \neq 0 \text{ ou } b' \neq$$

$$\frac{1}{z'} = \frac{a'}{a'^2+b'^2} - \frac{b'}{a'^2+b'^2}\, i$$

On retrouve évidemment la matrice inverse de celle attachée à z'

$$z' = \begin{bmatrix} a' & -b' \\ +b' & a' \end{bmatrix} \qquad \frac{1}{z'} = \frac{1}{a'^2+b'^2}\begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix}$$

On en déduit $\frac{z}{z'}$, $z' \neq 0$.

$$\frac{z}{z'} = z \cdot \frac{1}{z'}$$

Nombre complexe conjugué d'un nombre complexe donné.

C'est $\bar{z} = a - bi$ dès que $z = a + bi$

$$* f : \mathbb{C} \longrightarrow \mathbb{C}$$
$$z \longmapsto \bar{z}$$
$$a+bi \longmapsto f(z) = a - bi$$

* f est bijective.
* De plus, $\forall z \in \mathbb{C}$, $f \circ f(z) = z$ $\quad \boxed{\bar{\bar{z}} = z}$ (1)

f est donc involutive

$$* \quad z \xmapsto{f} \bar{z}$$
$$z' \longmapsto \bar{z}'$$
$$z + z' \longmapsto \overline{z + z'}$$

$$\overline{z + z'} = \overline{(a+a') + (b+b')i}$$
$$= a + a' - (b+b')i$$
$$= (a - bi) + (a' - b'i)$$
$$\overline{z + z'} = \bar{z} + \bar{z}'$$

$$\boxed{\overline{z + z'} = \bar{z} + \bar{z}'} \quad (2)$$

$$* \quad \overline{z z'} = \overline{(aa' - bb') + (a'b + ab')i}$$
$$= (aa' - bb') - (ab' + ba')i$$
$$\bar{z} \cdot \bar{z}' = (a - bi)(a' - b'i)$$
$$= (aa' - bb') - (ab' + ba')i$$

$$\boxed{\overline{z z'} = \bar{z} \ \bar{z}'} \quad (3)$$

f est donc un automorphisme involutif du corps $\mathbb{C}$.

Représentation géométrique d'un nombre complexe

On associe à $\mathbb{C}$, soit $\vec{P}$ vectoriel euclidien, soit P affine euclidien :

$b_1 : \mathbb{C} \longrightarrow \vec{P}$

$z \longmapsto \vec{w}$

$z = a + bi \quad \vec{w} = a\vec{u} + b\vec{v}$

$(\vec{u}, \vec{v})$ = base orthonormée de $\vec{P}$

$b_2 : \mathbb{C} \longrightarrow P = (O, \vec{P})$

$z \longmapsto M$

tel que :

$\vec{OM} = \vec{w} = a\vec{u} + b$

Remarques

A = image de z.

B = image de z'.

z = affixe de A.

z' = affixe de B.

$\vec{OA}$ = image de z, aussi.

z = affixe de $\vec{OA}$.

$z + z' = (a + a') + (b + b')i$

= affixe de $S \in P$

= " de $\vec{OS} \in \vec{P}$

$\vec{OS} = (a + a')\vec{u} + (b + b')\vec{v}$

$= \underbrace{(a\vec{u} + b\vec{v})}_{\vec{OA}} + \underbrace{(a'\vec{u} + b'\vec{v})}_{\vec{OB}}$

l'affixe de la somme est la somme des affixes.

$\overrightarrow{OS} = \overrightarrow{OA} + \overrightarrow{OB}$

y — axe des imaginaires purs

S $(z+z')$ — 2,5

1,5 — A (z)

(z') B

$\vec{v}$

3 — −2 — −1 — O — $\vec{u}$ — 1

axe des réels. — x

$\overrightarrow{BS}$ a, comme $\overrightarrow{OA}$, et comme A, pour affixe z

De plus : $\overrightarrow{OA} = \overrightarrow{OS} - \overrightarrow{OB}$

$(a, b) = (a + a', b + b') - (a', b')$

ou encore : $\overrightarrow{BS} = \overrightarrow{OS} - \overrightarrow{OB}$

donc :

affixe $\overrightarrow{BS}$ = affixe S − affixe B

12

odule d'un nombre complexe.

$z = a + bi$ $\quad\quad \bar{z} = a - bi$

$z\bar{z} = a^2 + b^2 = r^2$

$$|r| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2}$$

$r = |z|$

<u>Remarque</u>

$|z| = \| \overrightarrow{OM} \|$ si $M(z)$

Toutes les propriétés de $\|\vec{v}\|$, $\vec{v} \in \vec{E}$ espace vect. euclidien se retrouvent donc à propos de $|z|$, $z \in \mathbb{C}$ et en particulier : $|z_1 + z_2| \leqslant |z_1| + |z_2|$

(voir dans $\vec{E}$ inégalité triangulaire de Minkowski)

Par contre, avec l'opération $\times$, dans $\mathbb{C}$

$$\begin{aligned} |z_1 \cdot z_2| &= \sqrt{z_1 z_2 \cdot \overline{z_1 z_2}} \\ &= \sqrt{z_1 z_2 \cdot \bar{z}_1 \bar{z}_2} \\ &= \sqrt{z_1 \bar{z}_1 \cdot z_2 \bar{z}_2} \\ &= \sqrt{z_1 \bar{z}_1} \cdot \sqrt{z_2 \bar{z}_2} \\ &= |z_1| \, |z_2| \end{aligned}$$

$$\begin{aligned} \lambda : \mathbb{C} &\longrightarrow \mathbb{R}^+ \\ z_1 &\longmapsto |z_1| \\ z_2 &\longmapsto |z_2| \\ z_1 \times z_2 &\longmapsto |z_1 \cdot z_2| = |z_1| \times |z_2| \end{aligned}$$

λ est un homomorphisme (donc non bijectif) de $(\mathbb{C}, \times)$ vers $(\mathbb{R}^+, \times)$

Si l'on cherche le noyau de λ, c'est-à-dire l'ensemble des complexes dont l'image par λ est l'élément neutre de $\times$ dans ~~de~~ $\mathbb{R}^+$, on trouve tous les complexes de module 1, donc de matrices du type $\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ et $\alpha^2 + \beta^2 = 1$, $z = \alpha + \beta i$

Nous reconnaissons les matrices des rotations vectorielles de $\vec{P}$ (plan d'Argand-Cauchy)

Notons U ce noyau :

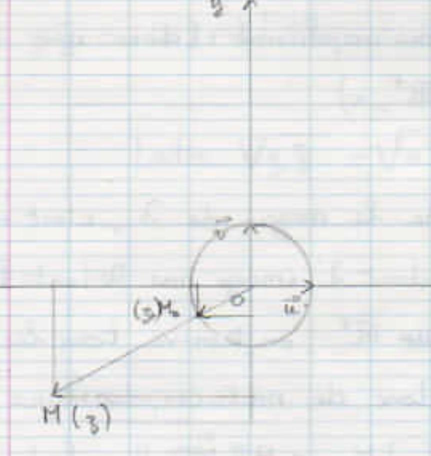
$$U = \{ z, z \in \mathbb{C} / |z| = \sqrt{\alpha^2+\beta^2} = 1 \}$$

Application

$\forall z \in \mathbb{C}, \quad \exists z_0 \in U / \quad z = |z| \, z_0$

$z = a + bi$

$z_0 = \frac{a}{|z|} + \frac{b}{|z|} i \qquad$ ou : $\quad z_0 = \frac{1}{\sqrt{a^2+b^2}} (a + bi)$



$\overrightarrow{OM} = \underbrace{\sqrt{a^2+b^2}}_{\in \mathbb{R}^+} \overrightarrow{OM_0}$

P

Remarque

$\overrightarrow{OM_0}$ n'est autre que l'unique vecteur unitaire de la droite affine (OM), qui est orienté comme $\overrightarrow{OM}$.

Distance définie sur $\mathbb{C}$

voir livre.

Racines carrées d'un nombre complexe

Soit Z donné, $Z \in \mathbb{C}$

$Z = a + bi$, $(a,b) \in \mathbb{R}^2$

Existe-t-il $z \in \mathbb{C}$ / $z^2 = Z$?

Posons $z = x + yi$, $(x,y) \in \mathbb{R}^2$.

Le problème revient à chercher s'il existe x et y réels

$(x+yi)^2 = a+bi$

$(x^2-y^2) + (2xy)i = a + bi$

$$\begin{cases} x^2-y^2 = a \\ 2xy = b \end{cases}$$

$$\begin{cases} x^2-y^2 = a \\ 4x^2y^2 = b^2 \\ \text{Sgn } xy = \text{Sgn } b \end{cases} \qquad \begin{cases} x^2+(-y^2) = a \\ x^2 \times (-y^2) = -\frac{b^2}{4} \\ \text{Sgn } xy = \text{Sgn } b \end{cases}$$

Posons $x^2 = X$

$-y^2 = Y$

X et Y, s'ils existent, sont les racines de l'équation :

$$X^2 - aX - \frac{b^2}{4} = 0 \qquad (1)$$

0.12

$\Delta = a^2 + b^2 \geqslant 0$; d'ailleurs les termes extrêmes sont de signe contraire $\vdash \exists (X', X'') \ / \ \underbrace{X'}_{-y^2} \leqslant 0 \leqslant \underbrace{X''}_{x^2}$

$\forall (a,b) \in \mathbb{R}^2 \vdash \forall Z \in \mathbb{C}$,

$\exists ! \ (X'', -X') = (x^2, y^2)$

$x^2 = X'' \vdash x = \mp\sqrt{X''}$

$y^2 = -X' \vdash y = \mp\sqrt{-X'}$

et on se souvient que

$\text{Sgn } xy = \text{Sgn } b$

Or le signe de b est connu (sauf si $b=0$) donc 2 associations et 2 seulement de signes

$b>0 \vdash \begin{cases} x = \sqrt{X''} \text{ et } y = \sqrt{-X'} \\ \text{ou} \\ x = -\sqrt{X''} \text{ et } y = -\sqrt{-X'} \end{cases}$

$b<0 \vdash \begin{cases} x = -\sqrt{X''} \text{ et } y = \sqrt{-X'} \\ \text{ou} \\ x = \sqrt{X''} \text{ et } y = -\sqrt{-X'} \end{cases}$

$z = x + yi$ $\quad \exists z'$ et z'', racines carrées de $Z = a + bi$

$z'' = -z'$

Si $b = 0$, $\quad X^2 - aX = 0$ voir (1)

$X(X-a) = 0$

$\begin{cases} X' = 0 \\ X'' = a \end{cases}$

* $a>0 \vdash x^2 = a$ et $-y^2 = 0$

donc $x = \mp\sqrt{a}$; $y = 0$

$\begin{cases} z' = \sqrt{a} + 0i = \sqrt{a} \in \mathbb{R} \\ z'' = -\sqrt{a} + 0i = -\sqrt{a} \in \mathbb{R} \end{cases}$

d'ailleurs : $Z = a + 0i = a > 0$

On savait que $z = \mp\sqrt{a}$

* $a<0 \vdash -y^2 = a$ et $x^2 = 0$

donc $x = 0$, $y = \mp \sqrt{-a}$

$$\begin{cases} z' = +i\sqrt{-a} \\ z'' = -i\sqrt{-a} \end{cases}$$

d'ailleurs $Z = a + \underbrace{b}_{0} i = a < 0$

car $Z = -(-a) = (-1)(-a)$

$= (-a)(-1)$

$= \underbrace{(-a)}_{>0} i^2$

$$\begin{cases} z' = -i\sqrt{-a} \\ z'' = i\sqrt{-a} = -z' \end{cases}$$

* $a = 0$ (et $b = 0$)

$X^2 = 0$

$X' = X'' = 0$

$x^2 = -y^2 = 0 \vdash x = y = 0 \vdash x + yi = 0 = z' = z''$

(et aussi $z'' = -z'$)

Équations du second degré

$ax^2 + bx + c = 0$ dans $\mathbb{C}$

$(a \neq 0)$

1°/ Supposons $(a, b, c) \in \mathbb{R}^3$; $x \in \mathbb{C}$.

* $\Delta = b^2 - 4ac \in \mathbb{R}$

$\Delta > 0$

alors $x = \dfrac{-b \pm \sqrt{\Delta}}{2a} \in \mathbb{R}$

* $\Delta = 0$

alors $x = -\dfrac{b}{2a} \in \mathbb{R}$.

* $\Delta < 0$

alors $\Delta = -\underbrace{(4ac - b^2)}_{-\Delta > 0}$

$4ac - b^2 \in \mathbb{R}^+$. On peut écrire $\Delta = (-\Delta)\, i^2$

$\Delta = z_1^2 = z_2^2$ et $z_2 = -z_1$

$z_1 = i.\sqrt{-\Delta}$ $z_2 = -i\sqrt{-\Delta}$

Les formules apprises dans $\mathbb{R}$ $(x \in \mathbb{R})$ sont encore valables dans $\mathbb{C}$, à condition de remplacer $\mp\sqrt{\Delta}$ par $+z_1$ ou $+z_2$

$$\left.\begin{aligned} x' &= \frac{-b + z_1}{2a} \\ x'' &= \frac{-b + z_2}{2a} \end{aligned}\right\} \text{avec } z_2 = -z_1$$

$\boxed{\Delta < 0}$

$$\boxed{x' = \frac{-b + i\sqrt{-\Delta}}{2a} \qquad x'' = \frac{-b - i\sqrt{-\Delta}}{2a}}$$

2°/ $(a, b, c) \in \mathbb{C}^3$

On peut, comme ci-dessus, calculer $\Delta = b^2 - 4ac \in \mathbb{C}$

Il existe z_1 et $z_2 \in \mathbb{C}$ telles que $z_2 = -z_1$

$$z_1^2 = z_2^2 = b^2 - 4ac$$

Alors, dans le corps $\mathbb{C}$, on peut utiliser les résultats classiques dans $\mathbb{R}$

$$\begin{cases} x' = \dfrac{-b + z_1}{2a} \\ x'' = \dfrac{-b + z_2}{2a} \end{cases} \quad \text{et } z_2 = -z_1$$

$\forall\ (a, b, c) \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}$
$*\ b^2 - 4ac \neq 0 \qquad \exists\, x', x'' \,/\, x'' \neq x'$
$*\ b^2 - 4ac = 0 \qquad \exists!\, x' = x'' = \dfrac{-b}{2a} \in \mathbb{C}$

On peut aussi reprendre la décomposition en carrés classique.

$$a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = 0$$

$$\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{4ac}{4a^2} = 0$$

$$\left(x + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2} \in \mathbb{C} \quad \text{avec} \quad \Delta = b^2 - 4ac$$

$$\exists\ z_1\ ;\ z_2 = -z_1 \ / \ z_1 = -z_2 = \frac{\Delta}{4a^2}$$

$$x + \frac{b}{2a} = \mp z_1 \qquad\qquad x = -\frac{b}{2a} \pm z_1$$

≃1952 A Boulbouris. (Mme Marotte en 1956)
1962 Lycée St Exupéry à St Raphaël